N° 683

___

# ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

TREIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 5 février 2008.

# RAPPORT D'INFORMATION

DÉPOSÉ

*en application de l'article 86, alinéa 8, du Règlement*

PAR LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE

*sur la mise en* **application de la loi n° 2006-64** *du 23 janvier 2006 relative à la* **lutte contre le terrorisme** *et portant dispositions diverses relatives à la* **sécurité** *et aux* **contrôles frontaliers**,

ET PRÉSENTÉ

PAR MM. ÉRIC DIARD, rapporteur et JULIEN DRAY, co-rapporteur

Députés.

___

## SOMMAIRE

Pages

Mesdames, Messieurs,

La loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers a été promulguée il y a un peu plus de deux ans. Adoptée en urgence, à la suite des attentats de Londres du 7 juillet 2005, cette loi n'avait pas pour objectif de révolutionner le droit français de l'antiterrorisme, mais plus modestement d'en compléter certaines lacunes, notamment en matière de police administrative.

En effet, la France, qui a été très tôt victime du terrorisme, a dû imaginer il y a quelques années une réponse à ce difficile défi, notamment avec la loi du 9 septembre 1986 qui fixe le cadre juridique et la méthode de lutte contre le terrorisme. Cette option française de l'antiterrorisme est fondée sur le primat de la détection précoce des réseaux terroristes, très en amont de l'organisation d'attentats : l'utilisation de l'incrimination de l'association de malfaiteurs en relation avec une entreprise terroriste ainsi que l'absence de frontières étanches entre services de renseignement et dispositif judiciaire sont des atouts qui expliquent en grande partie les succès de la France dans le domaine de la lutte contre le terrorisme.

Par ailleurs, la France a fait le choix d'apporter une réponse spécifique, donnant des droits exceptionnels et dérogatoires à la puissance publique, tout en restant dans un cadre protecteur des libertés individuelles, sous le contrôle des magistrats, même si ceux-ci sont spécialisés et centralisé au TGI de Paris. Grâce à ce système, nous avons su éviter les législations d'exception et le recours à des opérations ou à des pratiques illégales.

En 2005, au moment des débats parlementaires, la législation française était donc particulièrement étoffée suite aux interventions successives du législateur par-delà les clivages politiques, en 1986, 1996, 2001, 2003 et 2004. Pour autant, face aux mutations du terrorisme international, le Gouvernement avait jugé utile de donner de nouveaux outils aux services de lutte contre le terrorisme, particulièrement pour leur permettre de détecter plus en amont les réseaux terroristes, en dehors de toute commission d'infraction.

À l'assemblée nationale, le projet de loi avait été adopté avec les voix des députés de l'UMP et de l'UDF, les députés socialistes s'abstenant et les députés communistes votant contre.

La commission des Lois a estimé qu'il était aujourd'hui nécessaire de faire le point sur la mise en application de cette loi, dont le calendrier d'adoption avait été particulièrement rapide. Le Parlement ne saurait en effet se contenter d'une évaluation réalisée par le Gouvernement lui-même, telle qu'elle est prévue par l'article 32 de la loi du 23 janvier 2006 qui impose au Gouvernement de remettre chaque année un rapport sur l'application de la présente loi. D'ailleurs, aucun rapport n'a encore été remis au Parlement en application de l'article 32, deux ans après la promulgation de la loi : ce rapport serait en préparation et pourrait être finalisé d'ici la fin du premier trimestre 2008.

En outre, certaines des dispositions les plus novatrices de la loi (articles 3, 6 et 9) n'ont été adoptées qu'à titre temporaire et ne sont applicables que jusqu'au 31 décembre 2008. Le Parlement sera donc conduit à se prononcer sur la pérennisation de ces dispositifs et il importe qu'il dispose des éléments pour le faire dans de bonnes conditions.

● En premier lieu, il était souhaitable d'établir un **bilan sur la publication des décrets et circulaires nécessaires à la pleine application de cette loi**. Comme le montre le tableau figurant en annexe de ce rapport, ce bilan est relativement satisfaisant puisque la quasi-totalité des dispositifs prévus par la loi sont aujourd'hui utilisés par les services de lutte contre le terrorisme. Pour autant, certaines carences demeurent :

— une seule disposition de la loi, certes importante, ne peut aujourd'hui faire l'objet d'une mise en œuvre en raison de l'absence de publication d'un acte réglementaire : il s'agit de l'obligation pour les hébergeurs de site Internet et les fournisseurs d'accès à Internet de conserver et de transmettre aux services de lutte antiterroriste les données concernant l'identification des personnes à l'origine de la création de contenus en ligne (II de l'article 6 de la loi). Encore faut-il préciser que la publication de ce décret dépend de la publication préalable du décret d'application de l'article 6 de la loi du 21 juin 2004 relative à l'économie numérique. Compte tenu de l'utilisation croissante d'Internet par les réseaux terroristes, il est regrettable que cette disposition, applicable jusqu'au 31 décembre 2008, n'ait pas encore pu entrer en vigueur ;

— une autre disposition de la loi n'est pas appliquée par les services concernés dans l'attente d'une circulaire du ministre de la Justice et du ministre de l'Intérieur : cette disposition vise à permettre aux agents et officiers de police judiciaire de ne pas apparaître nominativement dans les affaires de terrorisme, mais seulement par un numéro d'immatriculation administrative. Cette disposition, très attendue par les enquêteurs, qui semblait pourtant d'application directe, a vu sa mise en œuvre retardée par la nécessité d'en préciser le régime juridique. Il est aujourd'hui urgent que la circulaire annoncée soit transmise le plus rapidement possible aux services de police et de gendarmerie intéressés ;

— enfin, un petit nombre de textes d'application prévus par la loi manquent, sans empêcher la mise en œuvre des dispositions qu'ils doivent préciser. Dans le domaine de la transmission des données de connexion aux services de lutte contre le terrorisme par les opérateurs de communication électronique, sont toujours attendus le décret précisant les tarifs des réquisitions administratives ainsi que le décret (nécessaire en l'absence de conventions conclues avec les opérateurs) fixant les modalités techniques de transmission des données. Dans un souci de sécurité juridique, la publication rapide de ces décrets s'impose.

● En second lieu, ce travail sur l'application de la loi du 23 janvier 2006 a pour but d'**évaluer les conditions de sa mise en œuvre concrète.** S'il est encore prématuré, et difficile compte tenu du sujet, de tirer un bilan de l'efficacité des dispositifs de la loi, il est néanmoins possible de donner un avis sur la mise en œuvre de ses principales dispositions emblématiques :

— en matière de **vidéosurveillance**, l'adoption de la loi a eu des résultats concrets, permettant l'installation de dispositifs dans des lieux qui ne pouvaient pas en être équipés jusque-là, et autorisant l'accès direct des services de police et de gendarmerie aux images. Votre rapporteur regrette simplement que la disposition permettant d'imposer la mise en place de systèmes de vidéosurveillance à des organismes susceptibles d'être menacés par le terrorisme n'ait pas fait l'objet d'application.

Le régime juridique de la vidéosurveillance a donc été modernisé et semble aujourd'hui adapté : son développement repose aujourd'hui principalement sur les moyens financiers qui seront dégagés, notamment dans le cadre du « plan national d'action de développement de la vidéoprotection » annoncé par la ministre de l'intérieur, de l'outre-mer et des collectivités territoriales en novembre 2007 ;

— le dispositif de **réquisition administrative des données de connexion** conservées par les opérateurs de communications électroniques, prévu à l'article 6, est pleinement applicable depuis le 2 mai 2007. Une plateforme de l'UCLAT, basée à Levallois-Perret, opère la centralisation nécessaire d'un dispositif qui satisfait aujourd'hui services utilisateurs, autorités de contrôle et opérateurs de communications électroniques. Les services de lutte contre le terrorisme disposent donc d'un outil utile pour surveiller les cellules terroristes très en amont, sans utiliser des dispositifs particulièrement intrusifs pour les libertés publiques comme les « écoutes téléphoniques » ;

— les traitements automatisés des données relatives aux **déplacements des voyageurs du transport aérien** sont progressivement mis en place, sur une base expérimentale. Ces traitements doivent encore être perfectionnés pour devenir réellement opérationnels. Mais ils constitueront sans doute dans les prochaines années un outil très utile dans le cadre de la prévention du terrorisme ;

— l'adaptation du **dispositif judiciaire de lutte contre le terrorisme** a répondu aux objectifs qui lui étaient assignés : améliorer le système à la marge, sans le remettre en cause. Ainsi, la centralisation de l'application des peines ou la possibilité de réunir une cour d'assises spécialement composée pour le jugement des mineurs accusés de terrorisme ont permis de répondre à des difficultés concrètes qui se posaient. Quant à la prolongation possible de la garde à vue en matière de terrorisme, pour 24 heures supplémentaires, renouvelable une fois, elle n'a été utilisée qu'une seule fois. En effet, les précautions prises par le législateur ont permis de donner un caractère tout à fait exceptionnel à cette mesure.

Dans le domaine de la lutte contre le terrorisme, évaluer l'efficacité des moyens de prévention et de répression est une entreprise très difficile. En effet, la circonstance que la France n'ait pas subi d'acte terroriste d'origine étrangère sur son sol depuis 1996 ne doit pas être perçue comme le signe que notre pays serait à l'abri d'une nouvelle vague d'attentats majeurs. La France reste en effet une cible de choix du terrorisme islamiste. C'est pourquoi, le dispositif de lutte antiterroriste doit se remettre en cause en permanence afin d'essayer d'avoir toujours un temps d'avance sur les terroristes.

# I. LES MESURES RELATIVES À LA VIDÉOSURVEILLANCE

## A. L'ASSOUPLISSEMENT DU RÉGIME D'AUTORISATION DES DISPOSITIFS DE VIDÉOSURVEILLANCE

Les enseignements tirés des enquêtes sur les attentats et tentatives d'attentats de Londres des 7 et 21 juillet 2005 avaient montré *a contrario* l'inadéquation de la législation française dans ce domaine. La modification de la loi du 21 janvier 1995, qui régit la vidéosurveillance en France, était donc au cœur des préoccupations qui ont justifié l'adoption de la loi du 23 janvier 2006. De fait, son cadre juridique est aujourd'hui modernisé, permettant d'envisager un développement significatif de la vidéosurveillance dans les prochaines années.

### 1. L'extension de la vidéosurveillance dans les lieux exposés au terrorisme

● L'article 10 de la loi du 21 janvier 1995, tel qu'il est issu de la loi du 23 janvier 2006, permet explicitement la prise en compte du risque terroriste comme motif légal d'installation d'un système de vidéosurveillance. En outre, les personnes privées exposées à des actes de terrorisme sont dorénavant autorisées à filmer la voie publique, « *pour la protection des abords immédiats de leurs bâtiments et installations* ».

La circulaire du 26 octobre 2006 relative à l'application des articles 10 et 10-1 de la loi n° 95-73 du 21 janvier 1995 modifiée d'orientation et de programmation relative à la sécurité insiste sur le fait « *qu'un tel recours à la vidéosurveillance ne trouvera sa justification que dans des cas nécessairement limités. Sont concernés les établissements constituant des cibles potentielles importantes pour des attentats, tels les lieux de culte, le siège social de certaines entreprises ou des grands magasins, sans que cette liste soit limitative* ». Il est également précisé aux préfets, chargés d'accorder les autorisations en matière de vidéosurveillance, que l'instruction réalisée par leurs services et par les commissions départementales de vidéosurveillance doit alors tenir compte de l'exposition réelle des établissements concernés à des risques de terrorisme *« qui ne sauraient être confondus avec des risques d'agression ou de dégradation s'inscrivant dans une problématique de délinquance ».*

D'après les informations communiquées à votre rapporteur, cette possibilité a cependant eu peu de traductions concrètes au cours de l'année 2006 : les ports autonomes de Dunkerque, de Strasbourg et, en Corse, plusieurs trésoreries principales et un pont routier en construction se sont équipés de vidéosurveillance dans le cadre de cette finalité. C'est à Paris que l'installation de la vidéosurveillance pour filmer la voie publique aux abords de sites sensibles a trouvé sa traduction la plus large puisque, depuis l'entrée en application de la loi du 23 janvier 2006, onze systèmes de vidéosurveillance « aux fins de lutter contre

les risques terroristes » y ont été autorisés. Ces autorisations concernent de grandes entreprises de communication et de transports de voyageurs, des lieux de culte et des bâtiments publics et également le réseau interdépartemental de la SNCF, soit 123 gares équipées à ce jour.

● Par ailleurs, la loi du 23 janvier 2006 a également introduit un article 10-1 dans la loi du 21 janvier 1995. Cette disposition prévoit que, dans certains lieux exposés à un risque terroriste (barrages, centrales nucléaires, infrastructures de transport…) la mise en place d'un système de vidéosurveillance n'est pas une simple faculté, mais peut être imposée par l'État. La circulaire précitée demande aux préfets de procéder à un recensement des sites susceptibles d'être concernés par cette obligation et « *d'établir avec le concours des services de police et de gendarmerie nationales, si les dispositifs de sécurité sont appropriés ou s'ils nécessitent d'être renforcés par un système de vidéosurveillance* ». Il est par ailleurs recommandé aux préfets de privilégier une démarche de négociation avec les responsables de ces sites, la disposition législative nouvelle étant donc considérée comme un moyen à utiliser en dernier ressort.

Le directeur des libertés publiques et des affaires juridiques du ministère de l'Intérieur a indiqué à votre rapporteur qu'il n'avait eu connaissance d'aucun cas d'utilisation de la nouvelle disposition législative. Il semblerait que certains préfets aient engagé des discussions avec des gestionnaires de sites sensibles, des transports publics principalement, mais qu'elles aient achoppé sur la question du financement des équipements de vidéosurveillance qui seraient rendus obligatoires. La loi ne prévoit en effet aucune disposition à ce sujet, ce qui empêcherait sa mise en œuvre. Pourtant, cette absence ne relève pas d'un oubli du législateur, mais d'une volonté assumée de celui-ci de ne pas faire peser sur l'État une dépense qui ne lui incombe pas, comme le montrent les travaux parlementaires. Le rapporteur de notre commission, M. Alain Marsaud avait ainsi justifié l'absence de compensation financière, considérant « *il n'est pas possible de transposer à la présente situation le raisonnement fait par le Conseil constitutionnel lorsqu'il a censuré la mise à la charge des opérateurs de télécommunications du coût des investissements nécessaires aux interceptions de sécurité* [(1)]*. En effet, contrairement à ce cas, les investissements à réaliser en matière de vidéosurveillance sont, d'une façon générale, réalisés volontairement par les personnes concernées : la mise en œuvre d'une procédure prescriptive permet de faire face à des attitudes de carence, qu'il ne faudrait pas encourager en participant au financement des systèmes de vidéosurveillance* » [(2)].

*(1) DC n° 2000-441 du 28 décembre 2000.*
*(2) Rapport n° 2681 (XIIème Législature) fait au nom de la Commission des Lois.*

Par ailleurs, un amendement [(1)] instituant une telle compensation avait été rejeté au Sénat. Dans ces conditions, la volonté du législateur, qui n'a fait l'objet d'aucune critique de la part du Conseil constitutionnel, est sans ambiguïté, et **doit conduire les préfets concernés à imposer des dispositifs de vidéosurveillance lorsque cela se justifie.**

### 2. L'amélioration de l'utilisation opérationnelle des systèmes de vidéosurveillance

● La loi du 23 janvier 2006 a prévu la **possibilité d'un accès direct aux images** des systèmes de vidéosurveillance appartenant à des tiers (collectivités locales, gestionnaires de transport public…) **par les services de police et de gendarmerie nationales**. Cet accès est fondamental pour permettre une utilisation efficace de la vidéosurveillance en matière de prévention et de répression de la délinquance et de la criminalité sous toutes ses formes. Jusqu'à la loi de 2006, les policiers et les gendarmes ne pouvaient avoir accès aux images prises par d'autres personnes que dans le cadre d'une procédure judiciaire ou s'ils étaient directement associés à l'exploitation du système de vidéosurveillance.

Cette possibilité est cependant très encadrée puisqu'elle doit avoir été prévue dans l'autorisation initiale délivrée par le préfet. De plus, il s'agit d'un accès limité aux agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales. Les conditions d'habilitation de ces derniers ayant été renvoyées au pouvoir réglementaire, la mise en œuvre de ces dispositions dépendaient de la publication du décret en Conseil d'État prévu par l'article 1er de la loi, intervenue dès le 28 juillet 2006 (décret n° 2006-929 du 28 juillet 2006). L'article 2 de ce décret précise que la désignation de ces agents est réalisée par « *le chef de service ou le chef d'unité à compétence départementale, régionale, zonale ou nationale* » où sont affectés les agents. Pour autant, la circulaire précitée indique que la désignation individuelle de ces agents est un acte distinct de l'indication, dans l'autorisation préfectorale, que la police ou gendarmerie peuvent accéder aux images : cette autorisation, ou un arrêté préfectoral pris postérieurement, ne doit donc pas comporter la liste nominative des agents qui peuvent accéder aux images et enregistrements, mais seulement la mention que cet accès est possible.

Cependant, cette faculté de transmission des images aux forces de l'ordre a été encore peu utilisée. En novembre 2007, sur les 230 communes équipées d'un dispositif de vidéosurveillance dans les zones de compétence de la police nationale, seules 53 avaient organisé le transfert d'images vers les services de police. Ainsi, dans le cadre du « plan national d'action de développement de la vidéoprotection » lancée par le ministre de l'Intérieur, de l'outre-mer et des collectivités territoriales, Mme Michèle Alliot-Marie, il a été décidé que le coût des raccordements, estimé à 4 millions d'euros, serait intégralement pris en charge

*(1) Amendement n° 61 présenté par les membres du groupe Union centriste UDF (séance du 15 décembre 2005).*

par l'État au travers du Fonds Interministériel de Prévention de la délinquance. Le financement du raccordement de 21 sites supplémentaires a été décidé dès le mois de novembre 2007, les préfets concernés s'étant vu déléguer une enveloppe d'un million d'euros. Le financement d'une deuxième série de raccordement devrait intervenir en février 2008.

Le plan d'action insiste aussi sur la nécessité de permettre aux forces de police d'accéder aux images des grands gestionnaires d'espace publics, tels que les centres commerciaux, les enceintes sportives ou les transports.

● L'augmentation de l'efficacité des systèmes pourra aussi reposer sur la **normalisation technique** des équipements imposée par la loi afin de disposer d'images de bonne qualité. Les systèmes de vidéosurveillance doivent désormais « *être conformes à des normes techniques définies par arrêté ministériel* ». À la suite d'une consultation des principaux opérateurs de vidéosurveillance, le ministre de l'intérieur a pris, dès le 26 septembre 2006, l'arrêté portant définition des normes techniques de vidéosurveillance qui portent à la fois sur la qualité, la conservation et l'exploitation des images ainsi que sur les fréquences d'enregistrement et la sécurité des réseaux.

La loi avait prévu que les dispositifs de vidéosurveillance devraient être mis en conformité avec les nouvelles normes dans un délai de deux ans, c'est-à-dire d'ici au 26 septembre 2008. Cependant, de nombreux utilisateurs de dispositifs de vidéosurveillance ont fait valoir que ce délai était trop bref et ne permettait pas d'amortir les investissements réalisés antérieurement. Pour répondre à cette préoccupation, un nouvel arrêté du 3 août 2007 a repris entièrement l'arrêté du 26 septembre 2006, en le complétant toutefois par trois annexes techniques : ainsi, le point de départ du délai de deux ans de mise en conformité a été retardé au 3 août 2007.

Ces normes permettront d'améliorer l'exploitabilité des images, c'est-à-dire de conforter la vidéosurveillance comme élément de prévention et comme outil d'élucidation des crimes et délits. La circulaire précise que si la loi a donné un délai de deux ans pour la mise en conformité des systèmes existants, les demandes d'installation nouvelles intervenues après la publication de l'arrêté doivent immédiatement se conformer aux nouvelles normes.

### 3. La nouvelle procédure d'autorisation provisoire

En cas d'urgence et de risque d'exposition au terrorisme, le préfet peut dorénavant accorder une autorisation provisoire d'installation d'un système de vidéosurveillance pour quatre mois, sans attendre l'avis de la commission départementale de vidéosurveillance.

Le ministère de l'intérieur [1] ne dispose pas de remontées systématiques de la part des préfectures lui permettant de savoir si cette disposition a été utilisée. En tout état de cause, il semblerait que cette procédure dérogatoire en urgence pourrait perdre sa raison d'être si les commissions départementales de vidéosurveillance étaient plus réactives. La périodicité de leurs réunions se situe en moyenne entre trois et quatre mois, même s'il y a des différences certaines entre départements, notamment entre ceux qui sont très urbanisés et ceux qui le sont moins. Afin de répondre à cette difficulté, Michèle Alliot-Marie a annoncé le 9 novembre 2007, lors de l'installation de la Commission Nationale de Vidéosurveillance présidée par Alain Bauer, qu'un « *décret en préparation prévoit qu'en cas de silence de la commission durant trois mois, l'avis est réputé reçu. Ceci permet au préfet de statuer sur une autorisation d'installation, dans le délai de quatre mois qui lui est imposé* ».

#### 4. La mise en œuvre de garanties supplémentaires

La loi du 23 janvier 2006 n'a pas uniquement étendu les capacités d'utilisation de la vidéosurveillance, mais elle a aussi amélioré son encadrement législatif et réglementaire :

— les autorisations sont désormais valables pour 5 ans, alors qu'elles l'étaient jusqu'alors sans limitation de durée : la circulaire précise que tous les arrêtés d'autorisation pris depuis la publication de la loi au journal officiel, le 24 janvier 2006, doivent comprendre un article précisant que l'autorisation a été délivrée pour une durée de 5 ans. Quant aux autorisations antérieures, elles arriveront donc toutes à échéance le 23 janvier 2011 ;

— les exigences en matière d'information du public ont été renforcées. L'article 3 du décret n° 2006-229 a ainsi précisé, conformément aux dispositions de la loi, les modalités d'information du public de l'existence d'un système de vidéosurveillance. Lorsqu'il s'agit de caméras filmant la voie publique, l'information est apportée « *au moyen de panonceaux comportant un pictogramme représentant une caméra* ». La circulaire indique que « *compte tenu des espaces vastes et ouverts où ces systèmes fonctionnent, les modalités d'information de leur présence doivent nécessairement être souples* ». Dans cette hypothèse, l'indication sur les panonceaux de l'identité du responsable du système de vidéosurveillance n'est pas exigée. En ce qui concerne les systèmes installés dans les lieux ou établissements ouverts au public, les exigences sont plus strictes puisque le décret précité demande que le format, le nombre et la localisation des affiches ou panonceaux soient adaptés à la situation des lieux et établissements. En outre, ces affiches ou panonceaux doivent indiquer les coordonnées du responsable du système de vidéosurveillance ;

---

*(1) À la suite de l'audition du directeur des libertés publiques et des affaires juridiques, celui-ci a indiqué qu'il allait modifier à l'avenir le questionnaire envoyé chaque année aux préfectures sur la vidéosurveillance afin d'obtenir des informations précises sur la mise en œuvre des dispositions introduites par la loi du 23 janvier 2006.*

— l'attribution d'un pouvoir autonome de contrôle à la commission départementale de vidéosurveillance a été décidée par la loi du 23 janvier 2006 : ses modalités de mise en œuvre ont été précisées par l'article 4 du décret n° 2006-929 du 28 juillet 2006. Ainsi, lorsqu'elle décide de mener une opération de contrôle, la commission peut désigner un de ses membres pour collecter des informations relatives aux conditions de fonctionnement d'un système de vidéosurveillance. La commission peut ensuite se réunir pour tirer les conséquences des contrôles, qui peuvent aller jusqu'à proposer au préfet la suspension de l'autorisation.

Ces dispositions ne se sont pas traduites par un développement des activités de contrôle des commissions départementales. En 2006, celles-ci ont procédé à 869 contrôles, dont 22 % ont donné lieu à la constatation d'infractions. En 2004, 942 contrôles avaient été opérés (dont 17 % ayant donné lieu à constatation d'infraction).

### B. LA MISE EN ŒUVRE À TITRE EXPÉRIMENTAL DU DISPOSITIF DE LECTURE AUTOMATISÉ DES PLAQUES D'IMMATRICULATION (LAPI)

L'article 8 de la loi du 23 janvier 2006 a consolidé les **dispositifs de surveillance automatique des véhicules** autorisés par la loi sur la sécurité intérieure du 18 mars 2003, mais jamais mis en œuvre. Désormais, ces appareils, les « LAPI » (système de lecture automatisée des plaques d'immatriculation), pourront être installés pour des raisons multiples, au-delà de la seule lutte contre le vol de véhicules. Les finalités de ces dispositifs ont en effet été définies par la loi de façon assez large (lutte contre le terrorisme, criminalité organisée, vol et recel de véhicule, délits douaniers…).

Concrètement, les LAPI pourront non seulement prendre la photographie de la plaque d'immatriculation des véhicules, mais également des occupants de ceux-ci. Cependant, les photographies des passagers ne seront accessibles aux services de police qu'à la condition que le traitement du numéro d'immatriculation fasse apparaître un croisement avec le fichier des véhicules volés ou mis sous surveillance (FVV) ou le système d'informations Schengen (SIS), ou bien dans le cadre d'une procédure judiciaire.

Le Gouvernement a fait le choix de mettre en œuvre ces dispositions de façon expérimentale. En effet, l'arrêté du 2 mars 2007 portant création, à titre expérimental, d'un traitement automatisé de contrôle des données signalétiques des véhicules autorise la mise en œuvre de tels traitements pour une durée de deux ans. Il est prévu une évaluation du dispositif à l'issu de cette expérimentation qui sera transmise à la CNIL.

Dans un avis rendu le 8 février 2007, la CNIL reconnaît que les finalités assignées aux traitements par l'arrêté sont celles qui ont été définies par le législateur au premier alinéa de l'article 26 de la loi du 18 mars 2003. Elle a néanmoins regretté que l'arrêté ne comporte « *aucune modalité précise d'application concernant les lieux d'implantation des dispositifs fixes ou mobiles et qu'elle autorise ainsi leur mise en œuvre en tous lieux du territoire* » ainsi que l'absence de définition des « *événements particuliers* » ou des « *grands rassemblements de personnes* » à l'occasion desquels ces dispositifs peuvent être utilisés. Elle a enfin souhaité une amélioration des dispositifs techniques d'effacement des données afin d'aboutir à la suppression totale et définitive des données au terme du délai de huit jours. Sur ce dernier point, M. François Giquel, vice-président de la CNIL, a indiqué que le directeur de cabinet de la ministre de l'Intérieur avait adressé, le 17 juillet 2007, un courrier à la CNIL précisant que le dispositif technique retenu permettait l'effacement effectif des données, au-delà de huit jours. La CNIL qui se félicite de cet engagement, en vérifiera le respect à l'occasion des contrôles qu'elle entend prochainement mener à l'égard des dispositifs LAPI d'ores et déjà opérationnels.

En effet, une expérimentation est actuellement en cours en Île-de-France par l'installation d'un dispositif embarqué de lecture automatisée des plaques à bord de véhicules sérigraphiés puis à terme, à bord de véhicules banalisés. Sont concernés 3 véhicules relevant de la préfecture de police de Paris et 3 véhicules relevant de la Direction départementale de la sécurité publique de Seine-Saint-Denis. Des résultats encourageants ont été enregistrés par les services de police parisiens : plus de 400 000 plaques d'immatriculation ont été lues en l'espace des quelques mois d'expérimentation en 2007, ce qui a permis d'identifier des dizaines de véhicules volés.

L'expérimentation actuelle doit être complétée par des dispositifs fixes en plusieurs points du territoire, notamment sur les points d'entrée très fréquentés de la ville de Paris.

## II. LA MISE EN PLACE D'UN VÉRITABLE DISPOSITIF DE POLICE ADMINISTRATIVE DE PRÉVENTION DU TERRORISME

### A. UN DISPOSITIF DE RÉQUISITION ADMINISTRATIVE DES DONNÉES TECHNIQUES LIÉES AUX COMMUNICATIONS DES TERRORISTES

La loi du 23 janvier 2006 a permis une meilleure prise en compte de l'utilisation croissante des nouvelles technologies par les réseaux terroristes, en facilitant le **contrôle de leurs communications électroniques** dans un cadre préventif. Les services spécialisés ont en effet un besoin vital d'accéder aux données techniques liées à l'utilisation de la téléphonie, fixe ou mobile, et de l'Internet. Avoir accès à ces données permet aux services de lutte contre le terrorisme d'identifier l'identité de l'ensemble des personnes appelées par un abonné, de connaître la date et la durée des communications, ainsi que la

localisation de tout possesseur d'un téléphone portable allumé, les « logs » de connexion Internet (numéro de protocole Internet, date et durée des connexions) et les données permettant d'identifier toute personne enrichissant le contenu d'un site Internet. Ces données n'ont pas trait au contenu des communications, mais elles sont très utiles pour suivre l'activité de réseaux terroristes présumés.

### 1. L'extension du champ d'application de l'obligation de conservation des données de connexion aux cybercafés et bornes wi-fi

La loi du 15 novembre 2001 relative à la sécurité quotidienne a posé le principe de la conservation des données de connexion des abonnés par les opérateurs de communications électroniques (opérateurs de téléphonie fixe et mobile et aux fournisseurs d'accès à Internet) pour les besoins d'une procédure pénale. Ces dispositions, inscrites à l'article L. 34-1 du code des postes et des communications électroniques, ont été modifiées par la loi du 23 janvier 2006, dont l'article 5 a étendu le champ.

En effet, cet article a permis d'allonger la liste des personnes soumises à l'obligation de conservation et de communication à la justice des données techniques. Y sont désormais soumises les « *personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit* ». Ces nouvelles dispositions étaient d'application directe, même si la relative imprécision de son champ d'application a été critiquée au cours des débats parlementaires. De nombreux parlementaires avaient alors estimé nécessaire qu'un décret dresse la liste précise des personnes soumises à cette obligation. Pour autant, le rapporteur de la commission des Lois, M. Alain Marsaud, avait clairement indiqué que cette disposition s'appliquerait aux gestionnaires de cybercafés, aux personnes qui offrent à leurs clients, dans un cadre public, ou à des visiteurs une connexion en ligne, tels les hôtels, les compagnies aériennes et fournisseurs d'accès à des réseaux de communications électroniques accessibles via une borne wi-fi.

En séance [(1)], le rapporteur avait interrogé le ministre délégué à l'aménagement du territoire sur le champ d'application de l'article. Celui-ci avait indiqué : « *Je serai très clair : nous visons d'abord les cybercafés, c'est-à-dire les personnes qui, au titre d'une activité professionnelle principale, offrent au public une connexion au réseau internet. (…) Les mairies, les universités, les bibliothèques ne sont pas concernées en principe, car leur activité ne consiste pas principalement à proposer des connexions Internet au public. Néanmoins, si l'on nous signalait que telle université ou telle bibliothèque devenait une sorte de cybercafé déguisé, alors elle pourrait entrer dans le champ des personnes soumises à cette obligation de conservation de données au titre de leur activité*

*(1) A.N, 1ère séance du jeudi 24 novembre 2005.*

*accessoire. (...) La définition proposée par le projet du Gouvernement n'appelle donc pas de précision par décret* ».

La circulaire du 21 juillet 2006 relative à l'application de la loi précise ainsi que « *les cybercafés et les bornes wi-fi seront désormais, notamment en ce qui concerne l'obligation de conservation de ces données, assimilés à des opérateurs de communication électronique* ».

Si les travaux parlementaires permettent manifestement d'établir la volonté du législateur, il semble qu'une incertitude demeure sur le champ d'application précis de cet article. Lors des auditions, la CNIL a ainsi rappelé qu'elle avait eu l'occasion de rappeler à plusieurs reprises son souhait que les dispositions législatives et réglementaires applicables soient plus précises. De fait, les services de la CNIL reçoivent une dizaine de demandes de consultation par semaine d'organismes, publics ou privés, qui cherchent à savoir s'ils relèvent des dispositions de l'article 5.

**Ainsi, même si la volonté du législateur est claire, il serait sans doute préférable qu'un texte, décret ou circulaire, décrive très précisément les organismes qui relèvent de l'obligation de conservation des données et ceux qui ne sont pas concernés. Il faut par ailleurs rappeler que le non-respect de cette obligation peut entraîner le déclenchement de poursuites pénales.**

Par ailleurs, si l'article 5 de la loi du 23 janvier 2006 était directement applicable, sa mise en œuvre dépendait pourtant indirectement de la publication d'un décret. En effet, il s'agissait donc d'allonger la liste des opérateurs soumis à des obligations particulières de conservation de données par la loi du 15 novembre 2001. Cependant, la nature des données à conserver et leur durée devaient être fixées par un décret en Conseil d'État, qui n'avait toujours pas été publié au moment de la promulgation de la loi du 23 janvier 2006, alors que plus de quatre ans s'étaient écoulés depuis l'adoption de la loi du 15 novembre 2001.

Le paradoxe consistant à étendre, en urgence, le champ d'application d'une disposition existant depuis 4 ans mais attendant toujours son décret d'application avait été largement évoqué pendant les débats parlementaires. Ainsi, il est probable que cette situation a permis d'accélérer le processus d'adoption du décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques. La liste des données à conserver, ainsi que la durée de conservation (un an) étant connues, les cybercafés et les bornes wi-fi doivent donc se soumettre aux obligations fixées par l'article 5 de la loi : c'est-à-dire conserver les données techniques générées par l'utilisation de leurs services

Il est important de préciser que la loi ou le décret n'ont fixé **aucune obligation d'identification des clients ayant recours à ces services**, ce qui constitue, selon les services de lutte contre le terrorisme, une sérieuse limite à l'utilité de la disposition. Ils considèrent en effet que la conservation des données de connexion des clients des cybercafés est peu utilisable dans la mesure où il

n'est pas possible d'identifier ces derniers. Ils soulignent également qu'ils n'existent aucune condition particulière pour proposer de tels services au public, contrairement à la législation italienne qui exige la sollicitation d'une autorisation préalable ainsi que l'identification de l'ensemble des clients. Ainsi, le cybercafé reste un moyen permettant de communiquer avec un risque assez faible d'être identifié.

### 2. La mise en place d'un régime de réquisition administrative des données de connexion

La loi du 15 novembre 2001, pleinement applicable depuis la publication du décret du 24 mars 2006, faisait obligation aux opérateurs de communications électroniques de conserver un certain nombre de données de connexion afin de les transmettre à la justice, sur réquisition, pour les besoins d'une procédure pénale. L'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique avait institué une obligation de même nature à la charge des hébergeurs de site Internet, mais toujours dans le cadre d'une procédure pénale.

Les nécessités de la lutte contre le terrorisme justifiaient la mise en œuvre d'une procédure de réquisition administrative des données de connexion, s'ajoutant à la procédure de réquisition judiciaire. En effet, la prévention d'actes de terrorisme exige de pouvoir disposer d'informations sur des personnes qui sont soupçonnées de participer à des réseaux terroristes, mais qui n'ont jusque-là fait l'objet d'aucune poursuite judiciaire. C'est pourquoi l'article 6 de la loi du 23 janvier 2006 a créé un dispositif, extrêmement encadré, d'accès de certains agents des services chargés de la prévention du terrorisme aux données conservées par les opérateurs de communication électronique et les hébergeurs de site internet.

#### *a) Une mise en œuvre rapide du dispositif de réquisition administrative des données conservées par les opérateurs de communications électroniques*

S'agissant des dispositions relatives à la réquisition administrative des données de connexion conservées par les opérateurs de communications électroniques, celles-ci sont désormais pleinement applicables grâce à la publication des textes suivants :

— le décret n° 2006-1651 du 22 décembre 2006 pris pour l'application du I de l'article 6 de la loi n° 2006-64 du 23 janvier 2006 a en effet permis une mise en œuvre rapide de ces dispositions. Il précise par exemple que les demandes de réquisition administrative ne peuvent être effectuées que par des agents habilités, désignés par le chef d'un service de police ou de gendarmerie spécialement chargés des missions de prévention des actes de terrorisme [(1)]. Il définit les

*(1) Conformément à la demande de la CNIL dans son avis sur le projet de décret (délibération 2006-219 du 28 septembre 2006), ce dernier fait directement référence à l'arrêté interministériel prévu par l'article 33*

informations à communiquer à l'appui des demandes de communication des données, ainsi que les modalités d'instruction des demandes par la « personnalité qualifiée », de contrôle par la Commission nationale de contrôle des interceptions de sécurité (CNCIS)…

— la décision n° 1/2006 du 28 décembre 2006 portant nomination de la personnalité qualifiée mentionnée à l'article L. 34-1-1 du code des postes et des communications électroniques était le complément indispensable du décret du 22 décembre 2006. En effet le législateur a prévu que les demandes de réquisition administratives sont soumises à la décision d'une personnalité qualifiée, placée auprès du ministre de l'intérieur. La désignation de cette personnalité qualifiée conditionnait donc la mise en œuvre de l'ensemble du dispositif. Le ministre de l'intérieur a donc présenté, comme la loi lui en fait l'obligation, une liste d'au moins trois noms à la Commission nationale de contrôle des interceptions de sécurité par deux lettres de saisine du 29 novembre et du 15 décembre 2006. La CNCIS a ensuite pu désigner M. François Jaspart, inspecteur général de la police nationale, en qualité de personnalité qualifiée pour une durée de trois ans. (1) Le nouveau dispositif est devenu pleinement opérationnel à partir du 2 mai 2007.

La désignation par la CNCIS avait été souhaitée par les parlementaires qui avaient adopté un amendement en ce sens, afin d'établir une réelle indépendance à la personnalité qualifiée, en dépit de son rattachement au ministre de l'Intérieur. Cependant, la CNCIS elle-même ne souhaitait pas disposer de cette prérogative, considérant qu'il était illogique que l'autorité de nomination de la personnalité qualifiée soit différente de son autorité hiérarchique, à savoir le ministre de l'Intérieur. Le président de la CNCIS, M. Jean-Louis Dewost, a cependant indiqué à votre rapporteur que le processus de désignation s'était déroulé dans d'excellentes conditions. Il a également considéré que l'indépendance démontrée par la personnalité qualifiée, qui s'est placée *de facto* sous l'autorité de la CNCIS, plaidait pour le maintien du mode de désignation retenu par la loi.

---

*de la loi qui fixe la liste de ces services. Cet arrêté, pris dès le 31 mars 2006, ouvre donc cette faculté aux services suivants :*

*— l'UCLAT ;*

*— Renseignements généraux : sous-direction de la recherche de la DCRG et les groupes, sections et unités de recherche spécialement chargés de la lutte contre le terrorisme au sein des directions régionales et départementales et de la direction des renseignements généraux de la préfecture de police ;*

*— Direction de la surveillance du territoire : services centraux spécialement chargés de la prévention et de la répression des actes de terrorisme et les services et unités territoriaux ;*

*— Police judiciaire : sous-direction antiterroriste, pôle de coordination des offices centraux, directions interrégionales et régionales de la police judiciaire ;*

*— Gendarmerie nationale : bureau de la lutte antiterroriste ; service technique de recherches judiciaires et de documentation, sections de recherches ;*

*— Offices centraux :Office central pour la répression du banditisme ; Office central pour la répression du trafic des armes, des munitions, des produits explosifs et des matières nucléaires, biologiques et chimiques ; Office central pour la répression de la grande délinquance financière ; Office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre ; Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication ; Office central chargé des personnes recherchées ou en fuite ; Office central de lutte contre les atteintes à l'environnement et à la santé publique.*

*(1) Par ailleurs, une décision n° 1/2007 de la CNCIS en date du 21 mars 2007 a permis la désignation de cinq adjoints à la personnalité qualifiée (J.O. du 25 avril 2007).*

### *b) La mise en œuvre satisfaisante du nouveau dispositif*

Dans la mesure où les dispositions de l'article 6 de la loi ont été adoptées à titre temporaire, jusqu'au 31 décembre 2008, il était important qu'elles rentrent rapidement en application, afin qu'il soit possible d'évaluer leur utilité.

Étudier le schéma type d'une demande de réquisition administrative de données de connexion permet de comprendre le fonctionnement du dispositif.

1ère étape : la demande initiale — Les fonctionnaires habilités des services de prévention du terrorisme, dont la liste est fixée par l'arrêté du 31 mars 2006, qui ont besoin, dans le cadre d'une mission de renseignement, de connaître les données techniques liées aux communications d'une personne adressent une demande, par message électronique crypté, à l'UCLAT, qui dispose d'une plateforme technique pour centraliser les demandes à Levallois-Perret. Ces demandes comportent des informations sur l'identité du demandeur, la nature précise des données demandées et enfin la motivation de la demande. L'UCLAT effectue un premier examen sommaire des demandes (vérification de l'existence des pièces justificatives, de l'identité du demandeur…).

M. François Jaspart, « personnalité qualifiée » estime le nombre de demandes quotidiennes entre 100 et 150 [(1)]. Ces demandes proviennent très majoritairement, pour environ les trois quarts, de la DST. La DCRG vient ensuite, loin devant les services à compétence judiciaire (Sous direction antiterroriste de la DCPJ, section antiterroriste de la préfecture de police, Gendarmerie nationale), ce qui est normal s'agissant d'une procédure de police administrative préventive. Il faut rappeler que seuls certains agents des services chargés de la prévention du terrorisme peuvent effectuer des demandes de réquisition des données de connexion : 551 agents de ces services ont reçu une habilitation en ce sens.

En ce qui concerne les données qui font l'objet d'une demande, la plus courante est l'identification d'un abonné à partir d'un numéro de téléphone (environ 70 % des demandes). Vient ensuite la liste des communications émises et reçues par un abonné qui permet d'établir l'environnement relationnel d'une personne (29,5 % des demandes). Les autres données pouvant faire l'objet d'une demande sont l'ensemble des informations concernant les abonnées d'un service de téléphone fixe ou mobile, ainsi que les informations concernant le trafic de ces communications, notamment la copie d'un document contractuel (0,25 %) ou des demandes relatives à la géolocalisation (0,04 % des demandes).

*(1) Chaque demande correspond à une opération distincte et non à une personne suivie par les services de lutte contre le terrorisme. En effet, une même personne peut engendrer plusieurs dizaines de demandes aux opérateurs.*

Depuis le 1er octobre 2007, les demandes peuvent également concerner les fournisseurs d'accès Internet (identification de l'adresse IP, des moyens de paiement utilisés…). Sur les mois d'octobre et de novembre, seules 59 demandes ont porté sur ce type d'informations. Cependant, compte tenu de l'évolution technologique (téléphone par Internet, communication par chat ou en utilisant des messageries électroniques…), il est probable que les demandes concernant ce type de données vont connaître une très forte augmentation dans les années à venir.

2ème étape : l'examen de la demande — L'UCLAT transmet ensuite la demande à la « personnalité qualifiée » qui instruit, elle–même ou l'un de ses adjoints, la demande dans des temps très brefs. La réponse est en effet toujours rendue dans la journée. En cas d'urgence, elle peut même être donnée pratiquement en temps réel.

La décision de la personnalité qualifiée s'impose, il ne s'agit en effet pas d'un simple avis. Cette décision peut être soit défavorable, soit défavorable, soit demander un complément de renseignements.

Sur l'ensemble de l'année 2007 (c'est-à-dire entre le 2 mai et le 31 décembre 2007), 27 701 demandes ont été présentées :

— 25 982 ont été validées par la personnalité qualifiée (soit un taux de 93,8 % d'acceptation) ;

— 243 demandes ont fait l'objet d'un refus. Les cas de refus portent principalement sur des demandes qui ne relèvent pas de la prévention, mais de la répression du terrorisme (et donc doivent utiliser les outils juridiques offerts par la procédure pénale), ou sur des demandes insuffisamment motivées qui ne font pas apparaître le caractère terroriste de la menace. Par exemple, une pratique rigoureuse de l'islam n'est pas un élément suffisant pouvant justifier la mise en œuvre de la procédure ;

— 1 476 demandes ont fait l'objet d'un renvoi pour informations complémentaires. Cette pratique reprend celle de la CNCIS en matière d'interceptions de sécurité (les « écoutes administratives »), elle illustre la qualité de la relation entre la personnalité qualifiée et la CNCIS.

3ème étape : la transmission des demandes aux opérateurs — La réponse de la personnalité qualifiée est transmise à l'UCLAT. Si celle-ci est positive, elle saisit alors les opérateurs de communication électronique qui sont tenus de lui transmettre les données dont ils disposent (l'obligation de conservation dure un an). Environ 90 % des demandes reçoivent une réponse dans un délai de 24 heures.

À la différence des agents des services de police et de gendarmerie, qui doivent être individuellement habilités, les personnels des opérateurs de télécommunication qui traitent ces demandes ne font l'objet d'aucune procédure préalable, même s'ils sont bien sûr tenus au secret professionnel. M. François

Giquel, vice président de la CNIL, a indiqué que cette dernière avait émis le souhait que le décret d'application institue une procédure d'habilitation pour ces personnels, que la loi n'avait d'ailleurs pas prévue.

4ème étape : la communication des données aux services demandeurs — Les données demandées sont transmises par les opérateurs à la plateforme technique de l'UCLAT, selon des modalités assurant leur sécurité, leur intégrité, et leur suivi qui devraient être définies par une convention ou, à défaut, par arrêté. En l'absence de convention ou d'arrêté, les opérateurs transmettent les données selon les modalités qu'elles choisissent, et qui ne correspondent pas aux standards informatiques utilisés par la police et la gendarmerie nationale, qui ne peuvent donc pas les exploiter de façon optimale (obligation de saisir manuellement les numéros de téléphone par exemple). Un projet d'arrêté imposant aux opérateurs le standard XML utilisé par la police et la gendarmerie est en cours de finalisation.

L'UCLAT transmet ensuite les données au service demandeur qui peut alors les utiliser pour la finalité qui en a justifié la transmission. Par ailleurs, le décret du 22 décembre 2006 (article R. 10-19 du CPCE) dispose que ces données sont enregistrées et conservées pendant une durée maximale de trois ans dans des traitements automatisés mis en œuvre par le ministre de l'intérieur et le ministre de la défense. M. François Giquel, vice-président de la CNIL, s'est inquiété que ce fichier n'ait pas fait l'objet d'une déclaration auprès de l'instance de régulation (1).

5ème étape : le contrôle par la CNCIS — L'article R. 10-20 du code des postes et des communications électroniques prévoit que les demandes approuvées par la personnalité qualifiée sont transmises dans les 7 jours à la CNCIS, selon des modalités fixées par l'arrêté du 10 mai 2007 du ministre de l'intérieur. Dans la pratique, le président Jean-Louis Dewost a précisé que la CNCIS recevait communication de l'ensemble des demandes formulées par les services de lutte contre le terrorisme, y compris les refus. En effet, la connaissance des refus est un élément essentiel permettant à la Commission d'évaluer la façon dont la personnalité qualifiée exerce sa mission : **il serait ainsi utile de clarifier juridiquement cette situation, afin de mettre le droit en accord avec la pratique** (2).

---

*(1) Il en est de même du fichier prévu par l'article R. 10-18 du CPCE concernant l'enregistrement et la conservation pendant un an des demandes et des décisions de la personnalité qualifiée.*

*(2) Cette pratique semble d'ailleurs davantage conforme à l'article L. 34-1-1 du code des postes et des communications électroniques que la rédaction retenue par l'article R. 10-20 du même code. En effet, l'article L. 34-1-1 dispose que « Les demandes accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité », sans préciser qu'il s'agit des seules demandes valisées par la personnalité qualifiée. Pour autant, il est vrai que l'article 27 de la loi n° 91-646 du 10 juillet 1991 semble limiter le pouvoir de la CNCIS aux demandes formulées auprès des opérateurs de communications électroniques, c'est-à-dire après validation par la personnalité qualifiée. Il serait utile de mettre en cohérence ces dispositions en précisant que la CNCIS est destinataire de l'ensemble des demandes.*

Plus globalement, le Président Dewost s'est félicité de la qualité de la relation entre la CNCIS et la personnalité qualifiée : celle-ci rencontre la Commission sur une base quasi-hebdomadaire, afin de confronter ses décisions avec les appréciations de la CNCIS. De la sorte, les grands éléments de la « jurisprudence » élaborée par la Commission dans le domaine des écoutes téléphoniques ont été repris par la personnalité qualifiée. Ainsi, le contrôle *a posteriori* prévu par la loi a une véritable incidence sur les décisions que prend la personnalité qualifiée.

La loi prévoit également que la CNCIS peut effectuer tous les contrôles qu'elle juge nécessaire et, en cas de manquement constaté, saisir le ministre de l'Intérieur d'une recommandation. Le président de la CNCIS estime que l'outil de la recommandation portant sur une demande en particulier n'est pas très adaptée, dans la mesure où il s'agit d'un contrôle *a posteriori* et que la recommandation ne pourra pas avoir de conséquences concrètes. Le travail au quotidien avec la personnalité qualifiée semble à cet égard beaucoup plus directement efficace. Pour autant, cette procédure reste utile car elle peut permettre d'attirer solennellement l'attention du ministre sur certains types de dysfonctionnement, permettant ainsi d'y mettre fin. En 2007, la CNCIS a ainsi émis une seule recommandation, portant sur une demande mal motivée, qui a permis une amélioration certaine des motivations des demandes. Dans ce domaine, la Commission est en effet plus exigeante pour les demandes qui ont un caractère très intrusif vis-à-vis des libertés publiques (géolocalisation ou liste des correspondants d'une personne) que pour celles qui portent uniquement sur l'identification d'un numéro de téléphone.

*

*  *

En somme, **le dispositif répond aux besoins qu'avaient exprimés les services de lutte contre le terrorisme** dans le cadre de la préparation de la loi du 23 janvier 2006. En effet, cet accès, encadré, aux données de connexion est tout d'abord un outil permettant de beaucoup mieux utiliser les moyens des services de lutte contre le terrorisme en facilitant le très important travail d'identification des personnes à suivre, et en écartant au contraire les personnes ne présentant pas de danger, tout en étant en relation avec une personne susceptible d'appartenir à un réseau terroriste. Dans le système précédent, afin d'exploiter un renseignement, les moyens à disposition étaient soit l'écoute administrative, moyen très intrusif et dont la procédure est particulièrement lourde, soit l'ouverture d'une information judiciaire. Désormais ces moyens peuvent n'être mis en œuvre que lorsqu'ils sont réellement nécessaires. Les autres atouts du dispositif sont sa rapidité et sa réactivité qui permettent l'accès à des informations très utiles pratiquement en temps réel.

Votre rapporteur constate un fort degré de satisfaction de la part de l'ensemble des personnes concernées par le dispositif, au-delà des premiers bénéficiaires que sont les services de lutte contre le terrorisme. Tout d'abord, les opérateurs de télécommunications électroniques se félicitent de la qualité de la relation avec l'UCLAT, considérée comme « *professionnellement agréable* ». En effet, l'UCLAT est le correspondant unique des opérateurs, contrairement au dispositif de réquisition judiciaire qui fait intervenir une multiplicité d'interlocuteurs potentiels : de la sorte, une relation suivie peut être établie permettant une plus grande efficacité du dispositif, mais également une plus grande sécurité des transmissions de données. Certes, les associations professionnelles du secteur ont fait part à votre rapporteur de certaines critiques, portant notamment sur l'insécurité juridique liée à l'absence de certains textes d'application. Cependant, les principales critiques des opérateurs et des fournisseurs d'accès portent sur la question de la compensation des coûts engendrés par les réquisitions, mais cette question ne porte pas directement sur les réquisitions administratives, mais sur l'ensemble des réquisitions, lesquelles restent très majoritairement (pour plus de 90 %) judiciaires.

La satisfaction autour du dispositif est partagée par l'autorité qui est chargée de son contrôle la CNCIS, laquelle estime qu'il a été mis en œuvre de façon très positive et se félicite des modalités de son propre contrôle.

### *c) Une carence préoccupante du pouvoir règlementaire s'agissant des données destinées à identifier l'origine des contenus mis en ligne.*

Si les dispositions concernant la réquisition des données techniques conservées par les opérateurs de communication électroniques ont connu une entrée en vigueur rapide, tel n'est pas le cas de celles qui devaient permettre l'identification des personnes ayant contribué à la création d'un contenu mis en ligne. Cette obligation de conservation devrait s'appliquer aux hébergeurs de site Internet et aux fournisseurs d'accès Internet (FAI). En effet, le II de l'article 6 de la loi du 23 janvier 2006, modifiant l'article 6 de la loi du 21 juin 2004 pour l'économie numérique, prévoyait un décret en Conseil d'État qui n'a pas encore été publié. Il s'agit d'ailleurs du seul acte réglementaire manquant pour l'application de la loi du 23 janvier 2006.

D'après les informations communiquées à votre rapporteur, le Gouvernement avait initialement envisagé un décret unique d'application de l'article 6 de la loi du 23 janvier 2006. De fait, le projet de décret transmis à la CNIL concernait l'application des I et II de l'article 6, alors que le décret du 22 décembre 2006 porte uniquement sur le I. Le Gouvernement a ainsi suivi l'avis de la CNIL [(1)] qui avait souhaité une entrée en vigueur différée du dispositif prévu au II. de la loi pour des raisons justifiées.

*(1) Délibération 2006-219 du 28 septembre 2006.*

Le projet de décret prévoyait en effet les modalités de transmission des données détenues par les hébergeurs de sites Internet de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires. Le problème vient de ce que ces données doivent être conservées en application de l'article 6 de la loi du 21 juin 2004, mais que leur définition, ainsi que la durée et les modalités de leur conservation devaient être fixées par un décret en Conseil d'État qui n'a toujours pas été publié. Dans ces conditions, comme le relevait la CNIL, le décret d'application de loi du 23 janvier 2006 ne peut intervenir avant la publication de celui de la loi du 21 juin 2004. En toute cohérence, il serait même préférable qu'un même décret fixe à la fois la nature des données à conserver par les fournisseurs d'hébergement et les modalités de leur transmission aux services chargés de la lutte contre le terrorisme.

Un nouveau projet de décret a donc été soumis à la CNIL, qui a rendu son avis le 20 décembre 2007. Interrogée par votre rapporteur, l'Association française des fournisseurs d'accès (AFA) a critiqué ce projet de décret, considérant que le champ des données à fournir était à la fois imprécis et trop étendu, pouvant même concerner des données qui peuvent être considérées comme relevant du contenu des communications (en-tête des messages électroniques). De plus, ils considèrent que l'obligation de conservation des données liées à l'usage d'Internet va contraindre les fournisseurs d'accès et hébergeurs de sites Internet à conserver des données qu'ils ne conservent pas actuellement pour des raisons commerciales, entraînant donc des surcoûts non compensés par les tarifs appliqués à ce type de prestation. Pour autant, la mise en œuvre rapide de ce décret, attendu depuis bientôt quatre ans est un impératif, compte tenu de l'usage croissant d'Internet par les membres des réseaux terroristes, au détriment des moyens téléphoniques.

L'avis de la CNIL soulève également un certain nombre de critiques (imprécision de la notion « d'identifiant » que les personnes concernées doivent conserver, insuffisance des dispositions sur les modalités de conservation des données…) qui portent principalement sur les modalités d'application des dispositions adoptées en 2004 (II. de l'article 6 de la loi n° 2004-575).

En ce qui concerne, la mise en œuvre des dispositions introduites par la loi du 23 janvier 2006, les observations de la CNIL reprennent celles faites à l'occasion de l'examen du décret n° 2006-1651 du 22 décembre 2006 (applicable aux opérateurs de communications électroniques). En effet ces dispositions sont relatives à la mise à disposition des données par les hébergeurs et les FAI aux autorités de lutte contre le terrorisme. La CNIL réédite donc ses observations sur la nécessité d'une habilitation des employés chargés de répondre aux demandes administratives de communication des données, sur sa volonté d'être saisie d'éventuels projets de décrets ou de conventions portant sur les modalités de sécurisation des transmissions… La CNIL rappelle également que la mise en œuvre de traitements automatisés des demandes réalisées et des données transmises devrait faire l'objet de la remise auprès d'elle d'un dossier de formalités préalables.

**Faut-il pérenniser les dispositions de l'article 6 de la loi du 23 janvier 2006 ?**

L'article 32 de la loi a prévu que certains des articles de la loi, dont l'article 6, seraient applicables jusqu'au 31 décembre 2008. Le caractère temporaire de ces dispositions se justifie par l'aspect novateur de certaines procédures dans des domaines qui intéressent les libertés publiques. Avant que ces dispositions ne soient éventuellement pérennisées par le Parlement, une évaluation de leur efficacité et de leur effet sur les libertés individuelles doit en effet être conduite.

La mise en œuvre très positive de la réquisition administrative des données de connexion des opérateurs de communication plaide incontestablement pour la pérennisation de ces dispositions au-delà du 31 décembre 2008. Quant au dispositif de réquisition des données conservées dans le cadre de la loi sur la confiance dans l'économie numérique, celui-ci n'étant pas encore entré en vigueur, il sera également nécessaire de prolonger son application afin de pouvoir évaluer son efficacité. Par ailleurs, les motivations qui ont justifié la mise en œuvre de ce dispositif, à savoir l'accroissement du risque terroriste, restent malheureusement toujours d'actualité.

Votre rapporteur considère donc nécessaire de prolonger l'application de la loi au-delà du 31 décembre 2008 : soit en pérennisant ces dispositions, soit, comme le souhaite la CNIL, en prolongeant leur application pour une nouvelle période temporaire de trois ans. En effet, au terme de cette période, il sera alors possible au Parlement d'avoir une vision générale de l'efficacité du dispositif, lui permettant de prendre une décision définitive.

### 3. Une occasion saisie pour clarifier la question de l'indemnisation des surcoûts supportés par les opérateurs

La loi du 15 novembre 2001 relative à la sécurité quotidienne avait prévu que les éventuels surcoûts à la charge des opérateurs liés à la conservation et à la communication des données techniques dans le cadre d'une réquisition judiciaire font l'objet d'une compensation financière. Cependant, dans la mesure où le décret prévu n'avait pas été publié, ce sont les opérateurs qui fixaient unilatéralement des tarifs qui étaient manifestement excessifs. Le niveau de ces tarifs s'était d'ailleurs traduit par une très forte augmentation des frais de justice dans la première moitié des années 2000 (+ 68 % entre 2002 et 2005).

Par ailleurs, il semble que cette délicate question de la fixation des tarifs applicables aux réquisitions soit en grande partie à l'origine de l'inertie du pouvoir réglementaire entre 2001 et 2006. Ainsi, afin d'assouplir le mécanisme de fixation des tarifs, l'article 18 de la loi du 23 janvier 2006 a prévu que le décret pourrait soit directement établir les tarifs, comme cela était le cas jusqu'ici, soit fixer les modalités de fixation de ce tarif. C'est cette deuxième option qui a été choisie par le pouvoir réglementaire, l'article 3 du décret précité du 24 mars 2006 précisant que les tarifs sont fixés par un arrêté du ministre de l'économie, des finances et de l'industrie et du garde des sceaux.

Ainsi, un arrêté du 22 août 2006 (J.O. du 1er septembre 2006) fixe le montant des tarifs de chacune des opérations réalisées par les opérateurs au profit des autorités judiciaires. La publication de cet arrêté, qui a entraîné une baisse des tarifs applicables, faisait partie d'un plan plus vaste mené par le ministère de la justice de maîtrise des frais de justice. Néanmoins, la nouvelle grille tarifaire (1) a largement contribué à la diminution des dépenses liées aux réquisitions auprès des opérateurs de communications : après une hausse de 242 % entre 1999 et 2004, et une hausse de 12,9 % en 2005, ces dépenses ont diminué de 44 % en 2006 (38 millions d'euros, contre 69 millions l'année précédente).

La grille tarifaire établie par cet arrêté fait cependant l'objet de critiques de la part des opérateurs de communications et des fournisseurs d'accès à Internet. Selon eux en effet, les tarifs appliqués prennent en compte uniquement le coût de la prestation opérée au cas par cas, sans prendre en compte les surcoûts induits par l'existence même d'un dispositif de réquisition des données qui contraindrait les opérateurs à des investissements supplémentaires (en matière de stockage des données à conserver notamment). Les fournisseurs d'accès estiment que les obligations légales et réglementaires leur imposent de conserver des données qu'ils ne conservent pas pour des raisons commerciales et craignent que cette situation n'empire dès que le décret d'application de l'article 6 de la loi pour la confiance dans l'économie numérique aura été publié. De plus, l'évolution technologique (développement de l'Internet sur téléphone mobile…) va entraîner un accroissement très significatif du stock d'informations à conserver, qui nécessitera de nouveaux investissements pour augmenter les capacités de conservation.

Certains opérateurs de communications et fournisseurs d'accès ont d'ailleurs attaqué pour excès de pouvoir l'arrêté du 22 août 2006, mais le Conseil d'État (2) n'a pas partagé leur argumentation, annulant uniquement une disposition bien spécifique de la grille tarifaire.

Dans le domaine des réquisitions administratives créées par l'article 6 de la loi du 23 janvier 2006, le décret n° 2006-1651 du 22 décembre 2006 (article R. 10-21 du code des postes et des communications électroniques) dispose que les surcoûts identifiables et spécifiques supportés par les opérateurs pour la fourniture de données techniques font l'objet d'un remboursement selon des modalités fixées par un arrêté conjoint du ministre de l'intérieur et des ministres chargés du budget et des communications électroniques. Les opérateurs de télécommunications ont signalé à votre rapporteur que cet arrêté n'avait pas encore été publié, ce qui n'a d'ailleurs pas empêché la mise en œuvre du dispositif de réquisition administrative des données de connexion le 1er mai 2007. Les prestations fournies ne sont pour autant pas réalisées gratuitement, mais le sont sur la base des tarifs des réquisitions judiciaires, ce qui ne semble pas poser de difficultés particulières, même s'il ne s'agit pas d'une solution satisfaisante. Pour des raisons de sécurité juridique, les

*(1) Avant même la publication de l'arrêté, des négociations avec les opérateurs avaient permis d'obtenir d'importantes réductions sur les tarifs pratiqués.*

*(2) CE, 7 août 2007, AFORS Télécom et autres.*

opérateurs souhaiteraient donc la publication de l'arrêté spécifique prévu par le décret du 22 décembre 2006.

### B. L'INTENSIFICATION DES CONTRÔLES TRANSFRONTALIERS

#### 1. L'extension des contrôles d'identité à bord des trains internationaux

L'article 3 de la loi du 23 janvier 2006 a modifié l'article 78-2 du code de procédure pénale afin d'étendre les possibilités de procéder à des contrôles d'identité systématiques à bord des trains internationaux, au-delà de la bande des vingt kilomètres. Désormais, les contrôles d'identité peuvent être effectués, d'une part, entre la frontière et le premier arrêt qui se situe au-delà de la zone des 20 kilomètres et, d'autre part, entre le premier arrêt situé à 20 kilomètres de la frontière et un autre arrêt situé dans la limite des 50 kilomètres suivants. Cependant, ces contrôles ne peuvent être opérés que sur des lignes internationales présentant des caractéristiques particulières de dessertes, fixées par arrêté ministériel. De même, la liste des arrêts concernés devait également être définie par cet arrêté.

Ainsi, ces dispositions sont devenues applicables avec la publication de l'arrêté du ministre de l'Intérieur du 26 avril 2006. D'après le directeur de la police aux frontières, cette disposition a contribué à l'augmentation du nombre de patrouilles mixtes (franco-belges, franco-allemandes, franco-italiennes ou franco-espagnoles) à bord des trains internationaux. En effet, avant la mise en œuvre de la loi, le temps disponible pour effectuer les contrôles d'identité, à savoir celui mis par le train pour atteindre le premier arrêt suivant la bande des 20 kilomètres, était trop bref pour réaliser des contrôles approfondis. En outre, la montée en puissance du service national de police ferroviaire, créé par l'arrêté du 27 juin 2006, a permis de dégager les moyens humains suffisants afin de procéder à ces contrôles d'identité.

Cependant, le directeur central de la police aux frontières a indiqué à votre rapporteur que la rédaction retenue en 2006 était assez restrictive puisqu'elle ne semblait permettre d'opérer des contrôles d'identités que dans le sens pays étranger/France, et non dans le sens inverse. La Cour d'appel de Bordeaux a par exemple annulé des contrôles d'identité pratiqués à bord de trains faisant la liaison entre la France et l'Espagne, considérant qu'il ne pouvait alors pas s'agir de contrôles migratoires. Dans la mesure où ces contrôles sont de plus en plus pratiqués par des patrouilles mixtes, cette distinction en fonction du sens de circulation semble relativement artificielle et pourrait faire l'objet d'une modification législative.

### 2. Le contrôle des déplacements des passagers du transport aérien

L'article 7 de la loi du 23 janvier 2006 a autorisé trois types de collectes des données des passagers du transport international de voyageurs, à l'exclusion de ceux voyageant au sein de l'Union européenne. Ces données peuvent ensuite donner lieu à des traitements automatisés permettant aux services de lutte contre le terrorisme et de lutte contre l'immigration clandestine de disposer d'une connaissance plus fine des déplacements internationaux.

#### *a) Le fichier national transfrontière (FNT)*

L'article 7 a tout d'abord permis la rénovation **du fichier national transfrontière**. Le FNT avait été créé par un arrêté du ministre de l'intérieur du 29 août 1991, mais il était peu utilisable car alimenté et exploité manuellement. La loi a ainsi autorisé son alimentation automatique à partir des bandes de lecture optique des documents de voyage et des données figurant sur les cartes d'embarquement et de débarquement.

L'arrêté du 3 novembre 2006 du ministre de l'intérieur portant modification de l'arrêté du 29 août 1991 relatif au traitement informatisé du fichier national transfrontière permet en théorie de collecter l'ensemble des données recueillies à l'occasion des contrôles frontaliers et de constituer un traitement automatisé à partir de cette base.

Cependant, en pratique, le dispositif n'a été mis en œuvre que pour les vols à destination d'un certain nombre de pays limitativement énumérés. En effet, la doctrine française de l'antiterrorisme est de privilégier la surveillance fine d'un certain nombre de cibles plutôt que d'opérer un contrôle généralisé de l'ensemble de la population par l'alimentation de gigantesques bases de données difficilement exploitables.

Le ministère de l'intérieur a donc indiqué à la CNIL que l'arrêté du 3 novembre 2006, qui est pourtant d'application générale, ne serait utilisé que pour quelques pays figurant sur une liste fixée par décision du ministre de l'intérieur et communiquée à la CNIL. Ainsi, cette dernière a reçu, par lettre du 2 mars 2007, la liste des 30 pays où le FNT rénové peut être mise en œuvre. En réalité, dans un premier temps, le ministère de l'intérieur a décidé de se concentrer sur cinq destinations « sensibles » [(1)] pour lesquelles l'ensemble des données des documents de voyage et des cartes d'embarquement sont recueillis au sein d'un traitement automatisé, et conservées pour une durée de trois ans, correspondant à la demande de la CNIL. Une autre demande de l'organisme de contrôle a été prise en compte puisqu'il n'y a pas d'interconnexion entre le FNT et le fichier des personnes recherchées (FPR) ou le système d'informations Schengen (SIS) [(2)].

---

*(1) Quatre de ces pays ont des liaisons aériennes régulières avec la France : Iran, Syrie, Yémen et Pakistan. Le cinquième pays est l'Afghanistan.*

*(2) La loi autorisait en effet une telle interconnexion, mais celle-ci n'était pas indispensable (contrairement au Fichier des passagers aérien) puisque le FPR et le SIS sont systématiquement consultés au moment du contrôle frontalier.*

L'avantage pour les services de lutte contre le terrorisme de disposer de ces données en temps réel est d'établir avec certitude l'arrivée d'une personne surveillée sur le territoire. Ces services ont donc commencé à s'équiper informatiquement afin d'avoir accès à ce traitement de données alimenté depuis février 2007. La DST, qui est principalement concernée, est ainsi reliée au système depuis décembre 2007.

***b) le fichier des passagers aériens (FPA)***

Le complément naturel du FNT est le fichier des **données collectées par les entreprises de transport international au moment de l'enregistrement** et dont elles disposent au moment de l'embarquement (données dites « APIS » [(1)]). Ces données sont certes moins fiables que celles du FNT, puisqu'elles sont recueillies par un tiers, le personnel des compagnies aériennes, mais elles permettent aux services d'anticiper, puisque ces données sont connues avant même le vol. Ainsi, la collecte et le traitement des données APIS ont également été autorisés par l'article 7 de la loi du 23 janvier 2006, lequel transposait en droit français la directive du 29 avril 2004 [(2)].

Le Gouvernement a choisi de mettre en œuvre ces dispositions novatrices de façon expérimentale : l'arrêté du 19 décembre 2006 du ministre de l'intérieur, du ministre de la défense et du ministre des transports crée en effet ce traitement automatisé pour une durée de deux ans à compter de sa publication au journal officiel (le 21 décembre 2006).

Comme pour le FNT, le nouveau fichier dénommé FPA (fichier des passagers aériens), est susceptible d'accueillir les données de l'ensemble des passagers du transport aérien. Cependant, dans un souci d'efficacité et de respect des libertés publiques, le choix a été fait de concentrer l'expérimentation sur les mêmes cinq pays que le FNT.

Le FPA est alimenté depuis mai 2007 par les données relatives aux passagers enregistrées dans le système de contrôle des départs des transporteurs aériens [(3)] à destination des pays concernés présents sur les aéroports de Roissy-Charles de Gaulle, Orly et Marseille Marignane. Ces données sont envoyées par les compagnies à la SITA [(4)] qui les transmet au poste de la Police aux frontières de Roissy. Les modalités de transmission de ces données ont été précisées par le décret n° 2006-1630 du 19 décembre 2006. En cas de manquements à leurs obligations de transmission des données, la loi prévoit une amende d'un montant maximum de 50 000 euros : bien que cette disposition soit applicable depuis la

*(1) Advance passenger information system.*

*(2) La directive 2004/82/CE du Conseil a contraint les États de collecter ces données dans le cadre de la lutte contre l'immigration clandestine. La France a choisi de permettre leur utilisation également dans le cadre de la lutte contre le terrorisme.*

*(3) Nom complet, date de naissance, nationalité, numéro et type de document de voyage utilisé, point de passage frontalier, heures de départ et d'arrivée, nombre total de personnes transportées, point d'embarquement initial.*

*(4) Société Internationale de Télécommunication Aéronautique.*

publication du décret n° 2006-725 du 22 juin 2006, aucune sanction n'a encore été prononcée à l'égard des compagnies aériennes, qui semblent faire preuve de bonne volonté.

Ces données sont ensuite acheminées au site du ministère de l'intérieur de Lognes (Seine-et-Marne) où est réalisée l'interconnexion avec le fichier des personnes recherchées (FPR) et le système d'informations Schengen (SIS). Si la mention « connu » apparaît, les services intéressés par cette information sont immédiatement avisés. Conformément au vœu de la CNIL, qui l'avait demandé dans son avis rendu le 14 septembre 2006, l'arrêté précise que cette mention est effacée au bout de vingt-quatre heures, alors que les autres données sont conservées pendant cinq ans [(1)]. En effet, l'inscription au FPR ou au SIS peut être évolutive dans le temps, son effacement rapide était donc nécessaire.

Les premiers mois de mise en œuvre ont montré que le dispositif nécessitait encore d'être perfectionné techniquement avant de devenir un outil incontournable de la lutte contre le terrorisme. Les principales failles du système sont :

— l'absence de prise en compte des vols avec escale : le système ne prend en compte que les vols directs en direction des cinq pays « cibles » ;

— les problèmes liés à la saisie des noms par les personnels des compagnies aériennes. En cas d'erreur au moment de l'alimentation du fichier, l'interconnexion avec le FPR et le SIS est en effet impossible. Une première solution pourrait consister à améliorer la formation des employés des compagnies aériennes. L'autre difficulté réside dans la transcription des patronymes de personnes dont la langue n'utilise pas l'alphabet latin ;

— le coût de la mise en œuvre de ce type de dispositifs qui en limite nécessairement la diffusion.

Conscient des améliorations à apporter au dispositif, le directeur central de la police aux frontières a indiqué à votre rapporteur que sa priorité était d'améliorer l'expérimentation actuelle avant de penser à la généraliser à d'autres pays. Un audit technique a d'ailleurs été demandé au Service des technologies de la sécurité intérieure du ministère de l'intérieur, qui permettra également de s'interroger sur l'opportunité de disposer de deux fichiers différents (FNT et FPA) concernant les mêmes pays.

***c) les données personnelles des voyageurs (PNR)***

Les **données enregistrées lors de la réservation du titre de transport, dites données PNR** *(passenger name record)* peuvent également être collectées et traitées dans le cadre de l'article 6 de la loi du 23 janvier 2006. Aucun traitement

*(1) Cependant, seuls les agents chargés de la lutte contre le terrorisme peuvent consulter ces données au-delà d'un délai de vingt-quatre heures. Dans le cadre de la lutte contre l'immigration clandestine, ces données ne sont donc consultables que 24 heures.*

enregistrant ces données n'a cependant encore été créé. Le chef de l'UCLAT a rappelé à votre rapporteur que le commissaire européen Franco Frattini avait présenté le 6 novembre 2007 une proposition de décision-cadre sur l'utilisation des données PNR, et qu'il semblait donc prématuré de mettre en place un dispositif de façon isolé, lequel pourrait ne pas être conforme à la future décision-cadre.

Votre rapporteur considère en outre qu'il est préférable que les services du ministère de l'intérieur se concentrent sur le perfectionnement des outils existants (FNT et FPA) avant de se lancer dans la mise en œuvre d'un nouveau traitement automatisé des données personnelles des voyageurs.

### C. L'ASSOUPLISSEMENT DES RÈGLES RELATIVES AUX FICHIERS DU MINISTÈRE DE L'INTÉRIEUR ET AUX FICHIERS INTÉRESSANT LA SÉCURITÉ NATIONALE

#### 1. L'accès aux fichiers du ministère de l'intérieur par les services chargés de la lutte contre le terrorisme

L'article 9 de loi du 23 janvier 2006 autorise les agents des services chargés de la lutte contre le terrorisme à avoir directement accès aux informations contenues dans un certain nombre de fichiers tenus par le ministère de l'intérieur (permis de conduire, passeports, cartes d'identité, fichiers relatifs aux étrangers…).

● La mise en œuvre de cet accès direct a nécessité la **mise à jour des actes réglementaires** concernant chacun des traitements automatisés dont l'accès a été autorisé par la loi :

— le fichier national des **immatriculations** est autorisé par les articles L. 330-1 et L. 330-2 du code la route. L'article R. 330-2 du même code prévoit l'accès direct aux informations contenues dans ce fichier par un certain nombre de fonctionnaires et de militaires (préfets, personnels du ministère des transports, policiers et gendarmes dans le cadre des contrôles routiers…). L'article 2 du décret n° 2007-86 du 23 janvier 2007 relatif à l'accès à certains traitements automatisés mentionnés à l'article 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers vient donc compléter l'article R. 330-2 du code la route : l'accès direct au fichier des immatriculations est désormais ouvert aux agents des services chargés de la lutte contre le terrorisme ;

— le système national de gestion des **permis de conduire** est autorisé par l'article L. 225-1 du code la route. L'article R. 225-4 de ce code fixe la liste des personnes ayant un accès direct à ce traitement : cet article a été complété par l'article 1er du décret n° 2007-86 du 23 janvier 2007 pour permettre la mise en œuvre des dispositions de la loi ;

— le système de gestion des **cartes nationales d'identité** a été créé par l'article 6 du décret n° 55-1397 du 22 octobre 1955. L'accès de certains services du ministère de l'intérieur et, sous certaines conditions, des services de police ou de gendarmerie, était prévu par les articles 10 et 11 du décret, qui ont donc été modifiés par le décret n° 2007-391 du 21 mars 2007 afin de permettre l'accès à ces données des agents des services de lutte contre le terrorisme ;

— le système de gestion des **passeports** (DELPHINE) est prévu par l'article 18 du décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques. Afin de permettre l'accès des services de lutte contre le terrorisme aux informations qu'il contient, l'article 4 du décret n° 2007-86 du 23 janvier 2007 a donc modifié le décret n° 2005-1726 du 30 décembre 2005 ;

— le système informatisé de gestion des **dossiers des ressortissants étrangers en France** (AGDREF) est organisé par l'article D. 611-1 du code de l'entrée et du séjour des étrangers et du droit d'asile (CESEDA). Les conditions de l'accès aux informations qu'il contient sont prévues par l'article D. 611-3, qui a ainsi été modifié par le décret n° 2007-87 du 23 janvier 2007 ;

— le traitement informatisé des empreintes digitales et de la photographie des ressortissants **étrangers qui ne remplissent pas les conditions d'entrée** sur le territoire français, prévu par les articles L. 611-3 à L. 611-5 du CESEDA, a été créé par le décret n° 2007-1136 du 25 juillet 2007. Pris après la promulgation de la loi du 23 janvier 2006, ce décret a donc pu prévoir dès l'origine l'accès aux données des agents des services de lutte contre le terrorisme ;

— le traitement informatisé des empreintes digitales et de la photographie des **demandeurs de visa (**BIODEV**),** prévu par l'article L. 611-6 du CESEDA, a été créé par l'article R. 611-8 du CESEDA. L'article R. 611-12 prévoit les modalités d'accès aux données de ce fichier, sa nécessaire modification a été opérée par l'article 3 du décret n° 2007-86 du 23 janvier 2007.

● Sur initiative sénatoriale, le dispositif de consultation des fichiers du ministère de l'intérieur avait été étendu à certains agents des services du ministère de la défense chargés de la prévention du terrorisme. La liste des services concernés devait être fixée par un arrêté conjoint des ministres de l'intérieur et de la défense. Cet arrêté a été signé le 27 juin 2006 (publié au J.O. du 12 juillet 2006), il concerne les services suivants : le service en charge des questions de protection et de sécurité de défense et les directions opérationnelles de la direction générale de la sécurité extérieure (DGSE), les sous-directions opérationnelles et les organismes extérieurs de la direction de la protection et de la sécurité de la défense (DPSD), la sous-direction des opérations de la direction du renseignement militaire (DRM).

● L'adaptation des actes réglementaires créant chacun des traitements était la condition juridique de l'application des dispositions de l'article 9. Pour que ces dispositions deviennent ensuite opérationnelles, il était nécessaire de réaliser les investissements techniques de raccordement permettant concrètement aux agents habilités d'accéder directement aux fichiers par une simple consultation informatique. Les principaux services de police et de gendarmerie chargés de la lutte contre le terrorisme peuvent avoir aujourd'hui accès aux fichiers des immatriculations et des permis de conduire.

Les services de lutte contre le terrorisme considèrent que cet accès direct à des fichiers, qui n'ont d'ailleurs pas un caractère sensible, est essentiel pour eux. Certes, ils pouvaient déjà avoir communication des données s'y trouvant en demandant à un agent de préfecture de consulter le fichier : cette pratique avait l'inconvénient d'être peu réactive, notamment en cas de besoin urgent la nuit ou le week-end. De plus, s'agissant d'affaires de terrorisme, il est important que l'identité de la personne faisant l'objet d'une demande de renseignement reste confidentielle, un accès direct aux fichiers est donc bien préférable.

Pour autant, ce droit nouveau attribué aux agents des services de lutte contre le terrorisme est très circonscrit : il s'agit uniquement d'une possibilité de consulter ponctuellement les fichiers, qui ne doit en aucune manière se traduire par la constitution d'un nouveau fichier, alimenté par des extractions des fichiers consultés. M. François Giquel, vice-président de la CNIL, a précisé que la Commission avait été très attentive à cette question et a reconnu que la mise en œuvre de cette disposition était conforme à la loi informatique et libertés. Par ailleurs, M. Christophe Chaboud, chef de l'UCLAT, a indiqué que les dispositifs informatiques de consultation des fichiers permettaient une « traçabilité » des demandes, permettant de connaître l'identité des auteurs des demandes et, au besoin, de vérifier le caractère justifié ou non de celles-ci.

### 2. La modification du régime juridique des traitements intéressant la sûreté de l'État, la défense ou la sécurité publique

L'article 13 de la loi du 23 janvier 2006, qui a modifié l'article 30 de la loi n° 78-17 du 6 janvier 1978, dite « informatique et libertés », dispense les demandes d'avis portant sur certains fichiers sensibles de comporter toutes les informations normalement obligatoires.

Les services de lutte contre le terrorisme estiment que cette modification répare un « oubli » de la loi du 6 août 2004 qui a modifié la loi de 1978. En effet l'article 19 de la loi de 1978 dans sa version d'origine origine prévoyait que les demandes d'avis ou les déclarations faites à la CNIL portant sur les fichiers intéressant la sûreté de l'État, la défense et la sécurité publique pouvaient ne pas comporter l'ensemble des informations habituellement requises sur le contenu et le fonctionnement des fichiers. Cette disposition a été supprimée en 2004, entraînant une inquiétude certaine de la part des services de renseignement qui craignaient qu'un excès de transparence ne permette aux terroristes de connaître

les méthodes de collecte et de traitement des renseignements relatifs à leurs activités.

De son côté, la CNIL estime que la suppression de cette disposition en 2004 devait s'apprécier en tenant compte de l'évolution du cadre de son contrôle prévu par cette même loi, qui a restreint le nombre de traitements devant faire l'objet d'une autorisation préalable. Pour autant, le texte définitif de l'article 13, élaboré en commission mixte paritaire, a tenu compte de certaines des objections de la CNIL en prévoyant que la liste des traitements concernés et des informations que les demandes d'avis sur ceux-ci doivent obligatoirement comporter sont fixés par décret en Conseil d'État, pris après avis de la CNIL.

Le décret n° 2007-914 du 15 mai 2007 dispose que huit actes réglementaires autorisant la création de fichiers gérés par la DST, la DGSE, la Direction du renseignement militaire (DRM) et la Direction de la protection et de la sécurité de la défense (DPSD) relèvent de l'article 13 de la loi du 23 janvier 2006.

Ce décret précise également que les demandes d'avis portant sur ces traitements doivent nécessairement comporter les mentions figurant à l'article 16 du décret n° 2005-1309 du 20 octobre 2005, tel que modifié par l'article 5 du décret n° 2007-451 du 25 mars 2007. M. François Giquel, vice-président de la CNIL considère que la liste des informations devant obligatoirement être fournies à la CNIL [(1)] donne globalement satisfaction à l'organisme de contrôle, même s'il regrette que la durée de conservation des données ne figure pas parmi les informations obligatoires.

### D. LE GEL ADMINISTRATIF DES AVOIRS FINANCIERS EN MATIÈRE DE TERRORISME

L'article 23 a introduit dans le code monétaire et financier un dispositif autonome permettant à l'autorité administrative de geler les avoirs des résidents communautaires. En effet, le Règlement du Conseil de l'Union européenne n° 2580/2001 du 27 décembre 2001 avait mis en place des mécanismes de gels des avoirs, qui n'avaient pas vocation à s'appliquer aux résidents communautaires.

Sur le fond, ces dispositions proposent un mécanisme particulièrement complet de gel des avoirs, définissant avec précision la nature des avoirs et ressources concernés ainsi que les effets de la mesure de gel tout en prévoyant que cette mesure, décidée par le ministre de l'économie, ne peut être prise que pour une durée de six mois renouvelable et qu'elle est susceptible d'engager la responsabilité de l'État. L'adoption de cet article a ainsi permis de compléter

*(1) L'identité et l'adresse du responsable du traitement ; ses finalités et sa dénomination ; les services chargés de sa mise en œuvre ; le service auprès duquel s'exerce le droit d'accès indirect ainsi que les mesures prises pour faciliter l'exercice de ce droit ; les catégories de personnes qui ont directement accès aux données enregistrées ; les destinataires ou catégories de destinataires habilités à recevoir communication des données ; les interconnexions, les rapprochements ou toute autre forme de mise en relation avec d'autres traitements.*

utilement la législation applicable en France en matière de lutte contre le financement du terrorisme. Les dispositions réglementaires nécessaires à l'application du nouveau dispositif ont été introduites par le décret n° 2007-545 du 11 avril 2007.

L'article L. 564-2 du code monétaire et financier prévoit que les décisions de gel des fonds pris par le ministre chargé de l'économie sont publiées au Journal officiel de la République française et exécutoires à compter de la date de cette publication. À ce jour, aucune décision ministérielle de gel des fonds n'a été prise dans ce cadre. Disposer d'un dispositif national de gel administratif des avoirs terroristes était le complément logique des dispositifs européen et « onusien ». Pour autant, la lutte contre le financement du terrorisme est bien plus efficace dans un cadre judiciaire qui permet des saisies définitives des avoirs, et non de simples gels : c'est cela qui explique que cet article de la loi du 23 janvier 2006 n'ait pas encore été utilisé.

## III. ADAPTER LE DISPOSITIF DE LUTTE JUDICIAIRE CONTRE LE TERRORISME

Déjà très complet au moment de la préparation de la loi du 23 janvier 2006, notre dispositif judiciaire de lutte contre le terrorisme est reconnu internationalement pour son efficacité. Ainsi, les modifications qui lui ont été apportées par cette loi, loin de remettre en cause sa philosophie, l'ont au contraire complété en parfaite cohérence avec les principes qui le fondent depuis 1986.

### A. LES DISPOSITIONS RELATIVES AUX INCRIMINATIONS

#### 1. La criminalisation de l'association de malfaiteurs terroriste dans certaines conditions

L'article 11 de la loi du 23 janvier 2006 a inséré un article 421-6 dans le code pénal afin de **criminaliser les associations de malfaiteurs ayant pour objet la préparation d'un attentat** portant atteinte aux personnes ou, en tout cas, susceptible d'entraîner la mort. Les personnes préparant de tels attentats sont dorénavant jugées par la cour d'assises spéciale et encourent jusqu'à vingt ans de réclusion criminelle, voire trente ans pour les dirigeants et organisateurs.

En effet, si le délit d'association de malfaiteurs en relation avec une entreprise terroriste était, et reste, particulièrement utile pour démanteler les réseaux, il ne permettait pas de prononcer des peines supérieures à dix ans à l'encontre d'individus potentiellement très dangereux. Ainsi, l'article 11 de la loi a permis de punir plus sévèrement ces comportements, sans modifier la pratique de notre système antiterroriste, fondé sur la détection précoce des cellules terroristes, qui sont démantelées avant de passer effectivement à l'action.

Depuis l'entrée en vigueur de la loi, aucune information judiciaire n'a été ouverte sur le fondement de l'article 421-6 du code pénal. Cela ne signifie pas que cet article est inutile, mais que, fort heureusement, aucun des groupes terroristes démantelés depuis cette date n'avait atteint un degré de préparation d'un attentat permettant d'utiliser cette incrimination. Les magistrats rencontrés dans le cadre de la préparation de ce rapport ont cependant fait observer que l'existence de cette incrimination aurait été très utile dans le cadre de réseaux démantelés avant le vote de la loi, notamment pour le « groupe de Francfort », qui fomentaient un attentat contre la cathédrale ou le marché de Noël à Strasbourg, en décembre 2000.

#### 2. L'extension du délit de non-justification de ressources

Une autre disposition concerne les incriminations, il s'agit de l'article 24 qui étend le **délit de non-justification de ressources** correspondant au train de vie à l'ensemble des infractions procurant un profit et punies d'au moins cinq ans d'emprisonnement.

D'après le directeur des affaires criminelles et des grâces, cette incrimination n'a pas encore pu être caractérisée dans une affaire de terrorisme, même si des enquêtes préliminaires sont en cours.

### B. LES DISPOSITIONS RELATIVES À L'ENQUÊTE ET À L'INSTRUCTION

#### 1. L'identification par un numéro d'immatriculation administrative des officiers et agents de police judiciaire chargés de la lutte contre le terrorisme

L'article 12 de la loi a autorisé, dans des conditions très strictes, les officiers et agents de police judiciaire affectés dans les services de lutte contre le terrorisme à **ne pas apparaître nominativement dans les procédures judiciaires**, mais sous un numéro d'immatriculation administrative délivré par le Procureur général. Cette disposition avait été proposée par le rapporteur de l'Assemblée nationale, alerté au sujet de cas concrets dans lesquels le nom d'enquêteurs avait été diffusé sur des sites Internet, mettant gravement en cause leur sécurité.

Pourtant, deux ans après la publication de la loi, cette disposition ne peut toujours pas être utilisée par les enquêteurs des services français de lutte contre le terrorisme. La circulaire du ministre de l'intérieur du 21 juillet 2006 précisait pourtant que l'article 12 était d'application immédiate, un décret en Conseil d'État étant uniquement prévu « *en tant que de besoin* ». Ces modalités de mise en œuvre se sont finalement avérées très peu efficaces. Le décret d'application n'étant pas obligatoire, il n'est pas anormal qu'aucun projet de décret n'ait été préparé dans les mois qui ont suivi l'adoption de la loi. Cependant, la disposition législative n'était manifestement pas assez précise, par exemple sur la question décisive de savoir si les enquêteurs seraient identifiés par un numéro d'immatriculation

unique, au risque de rendre l'anonymat recherché illusoire, ou par un numéro différent pour chaque procédure. Compte tenu de ces incertitudes, il a finalement été décidé d'adopter une disposition réglementaire (article 13 du décret n° 2007-1388 du 26 septembre 2007), qui précise les modalités d'application de ce dispositif, et notamment la possibilité d'utiliser un numéro d'immatriculation différent pour chaque procédure.

En dépit de la publication de ce décret, cette disposition n'est toujours pas utilisée, les services potentiellement intéressés préférant attendre la publication d'une circulaire interministérielle des ministres de l'intérieur et de la justice. Cette circulaire serait prête et devrait être publiée incessamment. D'ores et déjà, l'existence d'un cadre législatif a cependant permis à des enquêteurs espagnols, membres d'équipes communes d'enquête, d'apparaître en procédure sous leur numéro d'immatriculation.

**Il est regrettable que ces dispositions très utiles n'aient pas pu entrer en vigueur plus rapidement alors qu'elles étaient destinées à protéger les enquêteurs des services de lutte contre le terrorisme.** Ce retard plaide pour que le législateur indique clairement si un décret d'application est nécessaire, l'utilisation de l'expression « en tant que de besoin » étant source de confusion.

### 2. La prolongation de la garde à vue en matière terroriste

Au cours des débats parlementaires à l'Assemblée nationale, un amendement a permis une nouvelle **prolongation de la garde à vue** [(1)] **pour 24 heures supplémentaires renouvelables une fois,** sous des conditions très strictes : à savoir en cas de risque sérieux de l'imminence d'une action terroriste ou de nécessité liée à la coopération judiciaire internationale (article 17). Un sous-amendement de votre co-rapporteur avait précisé que cette prolongation devait être autorisée par le juge des libertés et de la détention, ne pouvant donc l'être par le seul juge d'instruction.

D'après les informations communiquées à votre rapporteur, aucune personne n'a été maintenue en garde à vue jusqu'au terme de la durée maximale théorique fixé par la loi du 23 janvier 2006, soit 144 heures (six jours). La nouvelle possibilité de prolongation n'a en effet été demandée qu'à une seule reprise, en février 2007, dans le cadre d'une enquête portant sur un groupe terroriste franco-belge formant des candidats au djihad en Irak. En effet, les nécessités de la coopération judiciaire franco-belge nécessitaient de disposer de plus de temps afin de pouvoir exploiter dans le cadre de la garde à vue le résultat des auditions parallèlement menées en Belgique : le parquet a donc saisi le juge des libertés et de la détention, qui a accordé une prolongation de la garde à vue pour 24 heures supplémentaires.

---

*(1) Pour les infractions de terrorisme de même que, pour les actes liés à la délinquance organisée, la garde à vue pouvait être prolongée au-delà de la durée maximale de droit commun de 48 heures pour une nouvelle période de 48 heures. Cette prolongation est autorisée soit, à la requête du procureur de la République, par le juge des libertés et de la détention, soit par le juge d'instruction.*

Votre rapporteur constate donc que les magistrats ont fait une utilisation mesurée de la nouvelle possibilité de prolongation de garde à vue, conforme à la volonté exprimée lors des débats parlementaires.

### 3. La question de la prolongation des écoutes ordonnées par le parquet dans le cadre d'une enquête préliminaire

La loi du 23 janvier 2006 a donc permis d'améliorer encore l'appareil procédural dont disposent les magistrats antiterroristes et les officiers de police judiciaire qui les assistent. Ceux-ci expriment donc leur satisfaction quant au dispositif de lutte antiterroriste dont ils disposent, qui leur semble globalement satisfaisant et complet.

Toutefois, un point de perfectionnement possible est apparu au cours des auditions, concernant les **pouvoirs du parquet au cours d'une enquête préliminaire.** L'article 706-95 du code de procédure pénale prévoit que le procureur de la République peut demander au juge des libertés et de la détention l'autorisation de mettre en place des « écoutes téléphoniques » dans le cadre d'une enquête de flagrance ou préliminaire portant sur des faits relevant de la « criminalité organisée » au sens de l'article 706-73 du même code, dont les actes de terrorisme. Toutefois, cette autorisation accordée par le JLD ne vaut que pour une durée de quinze jours, renouvelable une fois. Or, en matière d'enquête portant sur des actes de terrorisme, et en raison de la complexité de ces affaires, cette période d'un mois est insuffisante et oblige fréquemment le procureur de la République à ouvrir une information judiciaire, ce qui contribue à l'encombrement des cabinets des juges d'instruction. Le dispositif judiciaire de lutte contre le terrorisme est fondé sur la détection en amont des réseaux terroristes et sur leur démantèlement préventif, il en résulte que les enquêtes préliminaires diligentées par le parquet concernent des individus susceptibles d'appartenir à une association de malfaiteurs en relation avec une entreprise terroriste bien avant la préparation d'un attentat : le parquet a donc besoin de temps avant de pouvoir établir s'il est légitime de saisir un juge d'instruction.

C'est pourquoi, afin de concentrer l'instruction sur les affaires les plus complexes, **votre rapporteur souhaiterait que la durée maximale des écoutes mises en œuvre dans le cadre de l'enquête de flagrance ou préliminaire puisse être portée à deux ou trois mois à la demande du procureur de la République** et, bien évidemment, sur autorisation du JLD.

## C. LES DISPOSITIONS RELATIVES AU JUGEMENT ET À L'APPLICATION DES PEINES

### 1. La centralisation de l'application des peines

Alors que les lois adoptées à partir de 1986 avaient permis la mise en place d'une justice antiterroriste spécialisée et centralisée à Paris, que ce soit au

stade des poursuites, de l'instruction et du jugement, tel n'était pas le cas au stade de l'**application des peines**. La loi du 23 janvier 2006 parachève ainsi l'édifice juridictionnel centralisé en matière de lutte contre le terrorisme en confiant au juge de l'application des peines du tribunal de grande instance de Paris les décisions relatives aux condamnés terroristes. Le principe de la centralisation est en effet tout à fait adapté à ce genre de détenus qui, pour des raisons de sécurité, doivent fréquemment changer d'établissements pénitentiaires. De plus, compte tenu de la spécificité de ces détenus, il est préférable que le juge d'application des peines soit un spécialiste et connaisse bien les détenus dont il a la charge.

La loi avait prévu une application de la centralisation de l'application des peines des détenus terroristes dès le 1er mai 2006. À cette date, l'ensemble des établissements pénitentiaires accueillant des détenus dans des affaires de terrorisme n'était pas encore équipé de systèmes de vidéoconférence, le JAP national a ainsi dû faire neuf déplacements dans les premiers mois auprès des détenus. Au 1er janvier 2008, 41 des 47 établissements accueillant des détenus terroristes sont équipés en vidéoconférence, les autres sont en cours d'équipement.

L'avantage du dispositif tel qu'il fonctionne depuis bientôt deux ans est que le JAP national chargé du terrorisme a une très bonne connaissance des 150 dossiers dont il s'occupe (dont 30 dossiers de condamnés libres), ce qui lui permet de prendre des décisions éclairées.

Les auditions menées dans le cadre de ce rapport ont cependant fait apparaître une **lourdeur dans la procédure, liée à l'avis obligatoire demandé au JAP et au procureur du lieu de détention.** Dans la mesure où le choix a été fait de la centralisation pour tenir compte de la spécificité des détenus terroristes qui exige une connaissance fine de ceux-ci, il peut sembler inutile de demander un avis au JAP et au procureur du lieu de détention. Dans un souci de simplification, votre rapporteur considère que la sollicitation de cet avis devrait être une possibilité, mais ne devrait pas être obligatoire.

### 2. La création d'une cour d'assises pour mineurs spécialement composée de magistrats

L'article 15 de la loi du 23 janvier 2006 a étendu aux **mineurs** accusés de crimes terroristes les dispositions relatives aux jugements **par une cour d'assises spécialement composée de magistrats** (dont deux juges des enfants).

En l'absence de dispositions expresses, les mineurs éventuellement accusés dans des affaires de terrorisme ne pouvaient pas être jugés par la cour d'assises spécialement composées de magistrats du Tribunal de grande instance de Paris, instituée en 1986, et devaient donc être jugés par la cour d'assises des mineurs.

Cette lacune de notre législation avait pour inconvénient de faire juger des personnes accusées de terrorisme par une cour d'assises avec jury populaire, alors même que l'intention claire du législateur de 1986 était de faire juger ce type d'affaires par des magistrats professionnels, afin d'éviter des risques d'intimidation sur les jurés. De plus, l'impossibilité de faire juger des mineurs par la cour d'assises spécialement composée posait des problèmes pour des affaires concernant à la fois des majeurs et des mineurs : soit la justice pouvait décider de faire juger les accusés devant deux cours différentes, ce qui n'est pas de nature à favoriser une bonne administration de la justice, soit elle pouvait renvoyer l'ensemble des accusés devant la cour d'assises des mineurs. C'est cette dernière solution qui avait été retenue par le juge d'instruction dans l'affaire dite des « *clandestini corsi* » qui avaient dû renvoyer l'ensemble des neuf mis en examen pour des faits criminels devant la cour d'assises des mineurs de Paris dans la mesure où, parmi eux, deux étaient mineurs au moment des faits.

L'entrée en vigueur de la loi du 23 janvier 2006 a permis de remédier à cette situation. En effet, s'agissant d'une loi de procédure, celle-ci était immédiatement applicable à la répression des infractions commises avant son entrée en vigueur, en vertu de l'article 111-2 du code pénal. La chambre d'accusation de la Cour d'appel de Paris a donc pu faire application de ces dispositions et renvoyer, par un arrêt rendu le 7 mars 2006, l'ensemble des co-accusés, mineurs comme majeurs, devant la Cour d'assises des mineurs de Paris spécialement composé de magistrats.

Cette disposition de la loi du 23 janvier 2006 est donc loin d'être anecdotique alors que les spécialistes de la lutte contre le terrorisme observent que les réseaux terroristes, islamistes, basques ou corses, n'hésitent pas à recruter des personnes de plus en plus jeunes.

## IV. DES MESURES DIVERSES RELATIVES À LA SÉCURITÉ

### A. LES DISPOSITIONS DIRECTEMENT LIÉES À LA LUTTE CONTRE LE TERRORISME

#### 1. Les dispositions relatives aux victimes d'actes de terrorisme

Les articles 20 et 29 de la loi ont modifié le code des assurances afin d'améliorer l'indemnisation des victimes d'actes de terrorisme :

— l'article 20 a modifié l'article L. 126-1 du code des assurances afin d'étendre aux ayants droit étrangers de victimes de nationalité française d'un attentat commis en dehors du territoire français le bénéfice de l'indemnisation par le fonds de garantie des victimes des actes de terrorisme et d'autres infractions. Cette disposition législative a ainsi mis fin à une anomalie qui privait par exemple d'indemnisation le conjoint étranger d'une personne de nationalité française tuée dans un attentat à l'étranger. Cette disposition était directement applicable : les

ayants droit étrangers de personnes de nationalité française décédée en raison d'un acte de terrorisme commis à l'étranger peuvent donc formuler une demande d'indemnisation au Fonds de Garantie des victimes d'actes de terrorisme et d'autres infractions depuis le 24 janvier 2006 ;

— l'article 29 a modifié l'article L. 126-2 du Code des assurances en édictant une extension légale de garantie des attentats et des actes de terrorisme de toute nature dès lors que l'assuré est couvert par un contrat d'assurances de biens garantissant les dommages d'incendie. Il s'agissait de clarifier la situation juridique de certains contrats d'assurance n'offrant pas une couverture des biens totalement satisfaisante en cas d'actes de terrorisme, dès lors que certains cas d'exclusion (par exemple les dommages accidentels d'origine nucléaire ou bactériologique) pouvaient potentiellement s'appliquer en cas d'attentat terroriste. Cependant, la loi a prévu la possibilité de dérogation ou d'exclusion pour certains contrats concernant les grands risques : la liste de ces cas a été fixée par le décret n° 2006-1202 du 29 septembre 2006 définissant les dérogations et exclusions applicables aux contrats d'assurance concernant les grands risques en matière de couverture des dommages causés par un attentat ou un acte de terrorisme et modifiant le code des assurances [(1)].

Pour les risques « classiques », les nouvelles dispositions sont entrées en vigueur dès la publication de la loi du 23 janvier 2006 et ont pu immédiatement produire leurs effets puisqu'elles étaient applicables aux contrats en cours.

### 2. Le renforcement de la prévention par l'encadrement des activités de sécurité privée

● L'article 25 a permis de donner au préfet une plus grande marge d'appréciation pour délivrer ou non l'agrément aux personnes souhaitant exercer une activité de sécurité privée. Alors qu'il ne pouvait jusque-là consulter que les fichiers STIC et JUDEX, il peut dorénavant consulter également les fichiers de renseignement généraux, de la DST ou le fichier des personnes recherchées. Les personnes susceptibles d'apporter un soutien logistique à des activités terroristes n'ont pas nécessairement commis de faits inscrits dans les fichiers de police, mais peuvent néanmoins être connues des services de renseignement.

L'agrément pouvait déjà être refusé si « *la moralité de la personne ou son comportement apparaissent incompatibles avec l'exercice des missions pour lesquelles l'agrément est demandé* », indépendamment de toute commission d'infraction, mais le préfet disposait de peu d'éléments d'appréciation. Faute de pouvoir intervenir au niveau de l'agrément, il était parfois contraint de retirer l'agrément de personnes employées depuis de longues années, par exemple sur un site aéroportuaire, suite à un signalement fait par l'UCLAT.

---

*(1) Sont principalement concernés les contrats d'assurance de biens couvrant les dommages subis par les corps de véhicules ferroviaires, aériens, maritimes, lacustres et fluviaux ainsi que par les marchandises transportées.*

Cette disposition était d'application immédiate.

● L'article 26 a modifié le code de l'aviation civile afin de conditionner l'accès aux lieux de préparation et de stockage du fret à une habilitation délivrée par le préfet. De cette façon, suivant le même mécanisme que pour les personnes accédant aux zones réservées des aérodromes, des enquêtes administratives pourraient être diligentées sur les personnes employées dans ces zones lorsque leur entreprise est implantée en dehors des aérodromes.

Cet article permet la consultation des fichiers visés à l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés à l'exception des fichiers d'identification, c'est-à-dire, outre les fichiers STIC et JUDEX, les fichiers de personnes recherchées (FPR) ou les fichiers des services de renseignement (RG, DST).

Les modalités d'application de ces dispositions ont été définies par les articles 4 et 22 du décret n° 2007-775 du 9 mai 2007 relatif à la sûreté de l'aviation civile et modifiant le code de l'aviation civile.

### 3. Les mesures relatives à l'audiovisuel

L'article 22 de la loi du 23 janvier 2006 est issu d'un amendement de M. Philippe Houillon, pris pour répondre à une difficulté soulevée par M. Dominique Baudis, alors président du CSA. Les chaînes de télévision extra-communautaires diffusées sur le satellite Eutelsat relèvent de la loi française. À ce titre elles devaient être conventionnées par le CSA alors que cette procédure n'est pas adaptée pour des chaînes qui ne sont pas soumises à des obligations spécifiques, en dehors de celles imposées par la loi.

Dès lors, le conventionnement de ces chaînes constitue un handicap lorsque le Conseil supérieur de l'audiovisuel souhaite mettre un terme à la diffusion d'une de ces chaînes lorsque la programmation de celles-ci incite à la haine ou à la violence. Il s'était retrouvé face à une telle difficulté lors de l'affaire « Al Manar », chaîne de télévision du Hezbollah.

L'article 22 a donc entraîné la suppression du conventionnement de ce type de chaînes, permettant l'engagement de mesures et de sanctions appropriées dès constatation d'un manquement. Ces chaînes restent en effet soumises aux obligations de la loi et au contrôle du CSA qui peut notamment utiliser à leur égard les procédures prévues aux articles 42, 42-1 et 42-10 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

## B. LES DISPOSITIONS RELATIVES À LA SÉCURITÉ EN GÉNÉRAL

### 1. Les nouveaux dispositifs d'immobilisation des véhicules

L'article 4 de la loi a abrogé l'ordonnance n° 58-1309 du 23 décembre 1958 relative à l'usage des armes et à l'établissement de barrages de circulation par le personnel de la police pour le remplacer par un dispositif d'immobilisation des véhicules modernisé.

Les membres du personnel de la police, en uniforme, étaient autorisés à faire usage de tous engins et moyens appropriés tels que herses, hérissons, câbles, etc., pour immobiliser les moyens de transport quand les conducteurs ne s'arrêtaient pas à leurs sommations. Les herses et les « hérissons » sont des moyens lourds qui étaient de moins en moins utilisés car ils nécessitent une mise en place préalable.

L'article 4 modernise donc ce dispositif en le rapprochant des dispositions applicables à la gendarmerie nationale : désormais, les policiers peuvent procéder à l'immobilisation d'un véhicule non seulement qui ne répond pas à des sommations, mais également en cas de crime ou délit flagrant ou si le comportement du conducteur est dangereux. De plus, les matériels de nouvelle génération peuvent être utilisés de manière beaucoup plus souple, et au besoin projetés par les agents de la force publique au devant d'un véhicule en marche, sans provoquer au détriment du conducteur ni du véhicule de dommages liés à son utilisation.

La loi prévoyait que ces matériels devraient être conformes à des normes techniques définies par arrêté ministériel. Cet arrêté du ministre de l'Intérieur a été pris le 23 octobre 2006, il précise que les matériels doivent provoquer la décélération rapide puis l'immobilisation du véhicule par diminution progressive de la pression des pneumatiques, obtenue par l'usage de pointes adaptées.

Cependant, dans un souci de sécurité, l'article 3 de l'arrêté prévoit qu'avant mise en service, chaque type de matériel fait l'objet d'une expérimentation donnant lieu à évaluation par le service des technologies de la sécurité intérieure de la direction de l'administration de la police nationale. Au vu de cette évaluation, le directeur général de la police nationale fixe les conditions et les limites de l'emploi de chaque type de matériel.

### 2. L'interdiction administrative de stade

L'article 31 de la loi du 23 janvier 2006, issu d'un amendement de notre collègue Pierre-Christophe Baguet, a créé une mesure d'interdiction administrative de stade, prononcée par le préfet pour une durée de trois mois et pouvant être assortie d'une obligation de pointage au commissariat lors des matches.

Cette loi n'étant pas uniquement consacrée à la lutte contre le terrorisme mais aussi à des dispositions diverses relatives à la sécurité et aux contrôles transfrontaliers, elle avait semblé un vecteur législatif adapté, afin de mettre en œuvre cette mesure très attendue dans le cadre de la lutte contre le hooliganisme. Par conséquent, le pouvoir réglementaire s'est montré particulièrement prompt puisque le décret n° 2006-388 a été pris dès le 15 mars 2006. Ces dispositions ayant été complétées par la loi n° 2006-784 du 5 juillet 2006 relative à la prévention des violences lors des manifestations sportives, elles font l'objet d'une analyse de leur mise en œuvre dans le rapport de nos collègues Claude Goasguen et Christophe Caresche sur l'application de cette loi [(1)].

*(1) Rapport n° 396 (XIIIe législature).*

## OBSERVATIONS DE M. JULIEN DRAY, CO-RAPPORTEUR

En 2005, le groupe socialiste de l'Assemblée Nationale avait exprimé ses réticences et ses doutes à l'égard du bien-fondé et de l'opportunité de la loi relative à la lutte contre le terrorisme, qui était une loi de circonstance, même si elle n'était pas une loi d'exception. Cette loi fut adoptée dans l'urgence, sans prendre le temps et le recul qui auraient permis d'examiner sereinement ses dispositions. Il était pourtant manifeste que celles-ci pouvaient porter atteinte à la liberté de nos concitoyens, et que l'on pouvait douter de leur efficacité.

Si nous étions d'accord sur le principe d'adapter notre dispositif juridique et opérationnel de lutte contre le terrorisme aux évolutions de l'organisation et du *modus operandi* des groupes terroristes – notamment concernant la cyber-criminalité et ses évolutions récentes – nous étions plus circonspects sur le constat d'urgence mis en avant par le Ministre de l'Intérieur. Céder au sentiment d'urgence ou à la peur, c'est d'une certaine manière entrer dans le jeu des terroristes. *A contrario*, la réaffirmation du primat des valeurs républicaines doit être notre première réponse dans la lutte contre le terrorisme.

À cet égard, nous nous étions plus particulièrement inquiétés de plusieurs dispositions de cette loi. Sur la question du contrôle démocratique des services de renseignement par le Parlement, nous avons eu gain de cause via la création d'une délégation parlementaire dédiée.

En revanche, les questions du stockage des données informatiques, de la facilitation de l'accès des services de police et de renseignement à des fichiers jusque-là cloisonnés, ou encore du prolongement de la garde à vue en cas de suspicion de terrorisme, restent ouvertes et continuent, à nos yeux, à poser problème. Par ailleurs, l'extension de la vidéo-surveillance désormais installée paraît relever d'une fuite en avant, qui ne peut en aucun cas se substituer au travail de terrain.

Il s'agit pour nous d'un problème de principe, mais également de fait. Quelle est la véritable utilité de ces mesures ? Il apparaît aujourd'hui que l'histoire a rendu raison de nos doutes quant à l'argument de l'urgence : force est de constater que les services de police et de renseignement n'ont pas eu besoin de s'approprier tous les dispositifs dérogatoires mis en place par la loi du 23 janvier 2006.

Notamment, la possibilité de prolonger la garde à vue dans le cas de suspicions de terrorisme n'a été utilisée qu'une seule fois ; quant à l'extension du délit de non-justification de ressources, elle n'a pas encore été utilisée une seule fois. De façon générale, il est manifeste que les nouvelles – et très larges – latitudes d'action offertes par cette loi aux services de police et de renseignement

dépassent nettement les besoins réels. Et il faut rendre hommage au travail effectué par ceux-ci.

Nous ne pensons donc pas, par conséquent, qu'il faille, sous le coup d'une sorte de fatalisme juridique, et sous la pression d'hypothétiques menaces, considérer que les dispositions temporaires de cette loi (celles des articles 3, 6 et 9) doivent être prolongées, ou plus encore être définitivement entérinées.

## PROPOSITIONS DU RAPPORTEUR ET DU CO-RAPPORTEUR

— Inciter les préfets à imposer l'installation de systèmes de **vidéosurveillance** aux gestionnaires d'équipement confrontés à un risque de terrorisme, aux frais de ces derniers, comme le permet la loi du 23 janvier 2006 ;

— Publier un texte, décret ou circulaire, décrivant très précisément les **organismes qui relèvent de l'obligation de conservation des données** de connexion (cybercafés notamment) et ceux qui ne sont pas concernés (universités, bibliothèques) ;

— **Adopter rapidement les derniers textes réglementaires d'application du dispositif de réquisition administrative des données de connexion,** et particulièrement le décret relatif à l'identification des personnes ayant contribué à la création d'un contenu mis en ligne ;

— **Perfectionner les traitements expérimentaux des données des passagers du transport aérien (FNT et FPA)** avant de généraliser ces outils à de nouveaux pays ou de se lancer dans la mise en œuvre d'un nouveau traitement automatisé des données personnelles des voyageurs (PNR) ;

— Mettre en œuvre très rapidement le dispositif permettant l'**identification par un numéro d'immatriculation administrative des officiers et agents de police judiciaire chargés de la lutte contre le terrorisme.**

## PROPOSITIONS COMPLÉMENTAIRES DU RAPPORTEUR

— Prolonger l'application des dispositions temporaires de la loi **au-delà du 31 décembre 2008, en prolongeant leur application pour une nouvelle période temporaire de trois ans.** Au terme de cette période, il sera alors possible au Parlement d'avoir une vision générale de l'efficacité du dispositif, lui permettant de prendre une décision définitive ;

— Porter à deux ou trois mois, au lieu d'un mois actuellement, la durée maximale **des écoutes mises en œuvre dans le cadre de l'enquête de flagrance ou préliminaire** par le parquet ;

— Rendre **facultatif l'avis demandé au JAP et au parquet du lieu de détention** préalablement aux décisions du JAP national chargé des détenus terroristes.

## EXAMEN EN COMMISSION

Au cours de sa réunion du mardi 6 février 2008, la Commission a procédé à l'audition de Mme Michèle Alliot-Marie, ministre de l'intérieur, de l'outre-mer et des collectivités territoriales et examiné, en application de l'article 86, alinéa 8 du Règlement, le rapport sur la mise en application de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

*Après son exposé*, **M. Éric Diard,** *rapporteur*, a posé à la ministre les questions suivantes :

— La ministre souhaite-elle une pérennisation définitive des dispositions temporaires de la loi ou bien une prolongation de leur application pour une nouvelle période temporaire de trois ans ?

— Quand le décret permettant la mise en œuvre de l'obligation pour les hébergeurs de site Internet et les fournisseurs d'accès à Internet de conserver et de transmettre aux services de lutte anti-terroriste les données concernant l'identification des personnes à l'origine de la création de contenus en ligne pourra être publié ?

— La publication d'une circulaire précisant les conditions de mise en œuvre de la possibilité offerte aux agents et officiers de police judiciaire de ne pas apparaître nominativement dans les affaires de terrorisme, mais seulement par un numéro d'immatriculation administrative, est-elle prévue prochainement ?

— Le Gouvernement compte-t-il utiliser prochainement la possibilité offerte par l'article 2 de la loi anti-terroriste permettant d'imposer la mise en place de systèmes de vidéosurveillance à des organismes susceptibles d'être menacés par le terrorisme ?

— Où en est la mise en œuvre du « plan national d'action de développement de la vidéoprotection », annoncé par la ministre en novembre 2007 ?

— Les services de lutte contre le terrorisme disposent-ils aujourd'hui, notamment grâce à cette loi, des moyens juridiques nécessaires pour mener à bien leur mission ? Et au-delà des moyens juridiques, disposent-ils de moyens humains et financiers suffisants ?

**M. Julien Dray,** *co-rapporteur,* a rappelé que la loi du 23 janvier 2006 n'était ni une loi d'exception, ni une loi exceptionnelle. Elle n'était pas le *Patriot Act* mis en place par les Américains après les attentats du 11 septembre. Elle était avant tout une loi d'adaptation des différentes activités des services de sécurité visant souvent à inscrire dans la loi des pratiques qui existaient et à sécuriser les agents par rapport à ces pratiques. C'est pourquoi les députés socialistes n'avaient

pas manifesté une hostilité de principe à l'égard de ce dispositif en 2005 et en 2006. Ils avaient pris acte de l'état d'esprit qui présidait à l'élaboration de cette loi, qui était d'essayer de rendre plus opératoire l'action humaine des services de renseignement et de ne pas basculer dans le tout technologique – qui a montré son inefficacité par la suite dans un certain nombre d'opérations.

Le temps est venu d'évaluer le dispositif.

Les députés socialistes s'étaient demandés à l'époque s'il convenait d'adopter certaines mesures. Les faits montrent que plusieurs d'entre elles - notamment celles concernant la garde à vue – n'ont pas été beaucoup utilisées. Il peut être avancé qu'elles ne l'ont pas été parce que les circonstances n'ont pas conduit à en avoir besoin, alors même que l'activité terroriste n'a pas baissé. Si les services n'ont pas eu besoin d'avoir recours à ces mesures, c'est parce qu'ils ont souvent travaillé en amont, dans la recherche du renseignement – ce qui est la méthode de bon sens.

Les députés socialistes avaient également mis en garde contre certains dispositifs technologiques, notamment ceux sur la connexion des fichiers. Mais les interventions de la CNIL ont permis de « cadenasser » les procédures afin de garantir les libertés publiques et le respect d'un certain nombre de principes.

Tout d'abord, est-il nécessaire de prolonger l'expérimentation pour pouvoir faire une évaluation ? On peut en douter, au regard de l'expérience.

En réalité, soit on considère que le dispositif doit être maintenu et pérennisé, en l'intégrant dans le droit commun, soit, ce qui est préférable, on examine les dispositifs un à un, sans forcément les pérenniser, comme on peut le faire d'ores et déjà pour la garde à vue.

En second lieu, la question des opérateurs téléphoniques avait donné lieu à un débat très important. Le ministre de l'intérieur de l'époque avait stigmatisé les facturations et les délais exigés par les opérateurs téléphoniques. On avait l'impression d'être dans une situation d'urgence et que le ministre allait faire ce qu'il fallait pour « mettre au pas » les opérateurs téléphoniques. Force est de constater que tout cela n'était que discours. Les décrets n'ont pas été appliqués et tout continue comme avant, à la plus grande satisfaction des opérateurs téléphoniques.

Concernant la vidéosurveillance, des dispositions ont été prises dans la loi pour contraindre à son installation, mais il y a encore des réticences. Il ne s'agit aujourd'hui plus d'un débat philosophique, mais d'une discussion sur le caractère opérationnel ou non de la vidéosurveillance. Le bilan de la région Île-de-France en la matière n'est pas aussi bon que la ministre veut bien le dire. L'expérience de la ville de Londres, souvent mise en avant, n'est pas non plus très convaincante.

**Mme Michèle Alliot-Marie,** *ministre de l'intérieur, de l'outre-mer et des collectivités territoriales,* a félicité les rapporteurs pour la qualité du travail

effectué et s'est déclarée convaincue de la nécessité démocratique de procéder à une évaluation des lois.

La loi faisant aujourd'hui l'objet d'un rapport d'application a, comme l'a rappelé M. Diard, un peu plus de deux ans. Elle se voulait un moyen supplémentaire contre le terrorisme. Il existait déjà un certain nombre de dispositions en ce domaine mais le renforcement de la menace impliquait l'instauration de nouveaux moyens d'action. Ainsi, l'un des fondements de notre dispositif anti-terroriste reste l'incrimination d'association de malfaiteurs en relation avec une entreprise terroriste qui permet d'intervenir en amont du passage à l'acte. Elle est très utilisée, contre toutes les formes de terrorisme – islamiste comme de l'ETA.

La loi comporte un nombre important d'avancées. Certaines sont pérennes. D'autres ont été prévues, comme l'a souligné M. Diard, pour une durée limitée à trois ans : les contrôles d'identité dans les trains internationaux, la communication des données de connexion ou d'identification électroniques, et l'accès à des fichiers.

Concernant l'avenir de ces dispositions temporaires, la ministre précise qu'un article de la future LOPPSI qui sera soumise au Parlement avant l'été, prévoit la prorogation pour quatre ans, jusqu'au 31 décembre 2012 des articles 3, 6 et 9 du texte de 2006.

L'ensemble des dispositions de la loi de 2006, comme celles qui concernent les interceptions de véhicules, les aggravations de peines, l'habilitation des personnels intervenant en amont des zones réservées des aéroports, ou l'anonymat des procéduriers de police ou de gendarmerie n'appelle pas de commentaire particulier, étant précisé, sur ce dernier point, que le projet de circulaire a été finalisé par la direction générale de la police nationale et la direction des affaires criminelles et des grâces et est actuellement en cours de signature.

Certaines dispositions essentielles, très concrètes, de la loi de 2006, que les rapporteurs ont largement évoquées, méritent en revanche une attention particulière.

La première est la vidéoprotection, terme préférable à celui de vidéosurveillance, car le but des caméras est bien de protéger les citoyens contre, non seulement le terrorisme, mais également un certain nombre d'actes délictueux. Pour avoir écouté des maires de toute obédience politique au cours des derniers mois, la ministre a constaté que, contrairement aux dires de M. Dray, l'installation de caméras entraîne une baisse automatique et sensible de la délinquance dans les zones couvertes par celles-ci. Lors des derniers attentats de Londres, il a été manifeste que l'existence de caméras a permis d'éviter des conséquences beaucoup plus graves.

En dehors de la vidéosurveillance, les autres dispositions de la loi qui appellent des commentaires sont les communications électroniques ou téléphoniques, le traitement des données nominatives des passagers aériens – et, plus généralement, des personnes signalées qui sont amenées à se déplacer – et la lecture automatisée des plaques d'immatriculation.

Ces mesures dotent la France de nouveaux instruments efficaces, d'ores et déjà en application, qu'il revient au ministre de rendre toujours plus performants. C'est pourquoi, après les avoir exposés, elle s'est proposée de faire le point sur leur mise en œuvre et les développements qu'elle entend leur donner.

Il faut d'abord remarquer que, deux ans après l'adoption de la loi, l'essentiel des textes d'application est en vigueur.

Les articles 1 et 2 de la loi autorisent le recours à la vidéosurveillance comme outil de prévention des actes de terrorisme. Des arrêtés du 26 septembre 2006 et du 3 septembre 2007 imposent désormais des normes techniques qui permettent l'exploitation de l'image lors des enquêtes judiciaires.

La France a cependant encore beaucoup de retard, non seulement en comparaison avec d'autres pays, mais simplement au regard des besoins. C'est la raison pour laquelle la ministre veut multiplier par trois le nombre de caméras sur la voie publique, pour passer de 20 000 à 60 000, et qu'elle a parallèlement entrepris de systématiser, partout où cela est techniquement possible, le raccordement des centres de supervision des municipalités aux services de police ou de gendarmerie nationale, permettant ainsi une réaction immédiate et une interpellation dans les meilleurs délais.

Dès octobre 2007, le fonds interministériel de prévention de la délinquance a été sollicité à cette fin. Avant la fin du présent trimestre, 69 communes auront ainsi bénéficié de raccordements qui n'existaient pas avant et il y en aura 115 autres avant la fin de l'année. Au plan du soutien financier de l'État, ce ne sont pas moins de 30 millions d'euros qui viendront appuyer cette stratégie cette année.

La vidéoprotection ne concerne pas seulement les municipalités. Les transporteurs – RATP et SNCF principalement – vont accroître leur parc de caméras non seulement dans les gares et les stations mais également dans les trains, puisque des faits divers se sont malheureusement produits, montrant que la présence de caméras aurait pu sauver des vies humaines. Le développement des caméras se fera également dans les ports et les aéroports.

La ministre veillera à ce que tout cela se fasse en totale transparence et dans le souci de la protection des libertés publiques. C'est la raison pour laquelle tous les acteurs, transporteurs, collectivités locales et responsables du ministère de l'intérieur et même de la justice, se retrouvent dans différentes instances collectives, comme la commission nationale de la vidéo surveillance, ou le comité de pilotage stratégique dont la ministre a décidé la création. Sur le plan local, les

préfets animent eux-mêmes ce dispositif renouvelé, avec, pour souci, l'efficacité et la protection des libertés publiques.

Au vu des résultats des premiers échanges, qui se déroulent dans un esprit partenarial et constructif, il ne semble pas que l'application coercitive prévue par l'article 2 de la loi de 2006 soit nécessaire.

Le deuxième grand domaine est celui des communications électroniques ou téléphoniques.

La ministre s'est déclarée très attentive au problème de la cybercriminalité. C'est un enjeu fondamental dans la lutte contre le terrorisme. Les menaces récentes formulées contre la France sur des sites bien connus montrent l'actualité de cette préoccupation. Les terroristes utilisent Internet pour passer leurs messages. Ces messages peuvent avoir des effets sur des esprits faibles et les conduire à se transformer en terroristes potentiels, qu'il est difficile de repérer.

Les terroristes, qui utilisent Internet pour faire circuler des informations, ont pris depuis longtemps l'habitude de communiquer par Internet à partir de bornes wi-fi ou de cybercafés. C'est pourquoi les articles 5 et 6 fixent les obligations de ces établissements, des opérateurs de communication électronique, et des hébergeurs de sites Internet, au bénéfice des services chargés de la lutte antiterroriste. Il est regrettable que ces obligations légales, notamment en matière de conservation d'un certain nombre de données, ne soient pas toujours respectées par ces opérateurs.

Le décret prévu à l'article 6 II *bis* a été présenté à la CNIL au début de l'automne. L'avis rendu par cette instance le 20 décembre contenait plusieurs observations, et les conditions de leur prise en compte doivent prochainement être décidées au cours d'une réunion interministérielle, précédant la saisine du Conseil d'État.

Les deux autres textes cités par M. Diard, du niveau de l'arrêté, sont en phase de finalisation. Ils concernent le tarif des réquisitions administratives et les modalités techniques de transmission des données par les opérateurs. Ce dernier arrêté fait l'objet de demandes de précisions du secrétariat général de la défense nationale, qui vont être prises en compte.

Mais sur le plan opérationnel, l'ensemble du texte est maintenant en application.

Ainsi, l'article 6 prévoit une structure permettant aux services de renseignement d'accéder aux données de trafic téléphonique et électronique auprès des opérateurs et des hébergeurs de sites Internet.

La plateforme UCLAT a été créée à cette fin. Opérationnelle depuis le 2 mai dernier, elle permet de traiter les demandes de transmission aux services de

renseignement d'informations sur les échanges électroniques et téléphoniques. Elle est devenue rapidement un instrument incontournable pour les services de renseignement. Elle permet aujourd'hui à 551 fonctionnaires spécifiquement habilités, issus de sept directions, d'obtenir des données techniques d'identification et de connexion de la part d'opérateurs ou d'hébergeurs de sites Internet, dans un délai de 24 à 48 heures.

La procédure suivie est à la fois efficace et respectueuse des libertés individuelles. Toute demande de la part des services est validée par la « personnalité qualifiée », nommée par la commission nationale de contrôle des interceptions de sécurité (CNCIS). Cette dernière reçoit chaque semaine le bilan des demandes, et peut formuler des observations qui sont aussitôt prises en compte.

Le troisième grand domaine de la loi de 2006 est le suivi des personnes recherchées. L'article 7 de la loi permet le traitement automatique de données nominatives de passagers extérieurs à l'Union européenne. Dans l'esprit de ce texte, le fichier des passagers aériens – FPA –, interconnecté avec le fichier des personnes recherchées – FPR –, a été créé. Il recueille les données APIS - *Advanced Passengers Information System* – envoyées électroniquement par les compagnies aériennes.

Le fichier des passagers aériens est actuellement en cours d'expérimentation pour deux ans sur les aéroports de Roissy CDG, Orly et Marseille. Il permet de détecter en amont les passagers recherchés, et de garder une trace des voyageurs en provenance ou à destination de cinq pays sensibles : l'Afghanistan, le Pakistan, l'Iran, le Yémen et la Syrie.

Le renforcement des contrôles aux frontières aériennes est une priorité ; il devra encore être perfectionné en l'élargissant à un plus grand nombre de pays sensibles.

Il faut aussi tenir compte du fait que les personnes que les services de sécurité ont en face d'eux savent ce que ces derniers font et détectent, et vont donc essayer de contourner les mesures mises en place. Par conséquent, même si c'est techniquement difficile, il faudra, en plus d'élargir la liste des pays sur lesquels doit s'appliquer le système de contrôle, prendre en compte les vols indirects. Certaines personnes dangereuses passent, pour se rendre en Afghanistan ou au Pakistan, par la Suisse et ne figurent donc pas sur les fichiers français. La tâche n'est pas facile mais elle est indispensable pour que les services de sécurité soient efficaces.

La présidence française de l'Union européenne à partir du 1er juillet 2008 devra être mise à profit pour essayer d'accélérer l'adoption d'une décision cadre permettant aux services de sécurité français d'effectuer des croisements avec les fichiers PNR – *Passenger Name Record* – mis en place dans l'espace Schengen

pour essayer de mutualiser les connaissances en la matière. Leur champ d'application est plus large que celui des fichiers APIS.

Un autre dispositif important est celui de la lecture automatique des plaques d'immatriculation, dit LAPI, prévu à l'article 8. L'utilisation de ce dispositif a, par exemple, permis à la Grande-Bretagne d'identifier certains réseaux terroristes. Ce système permet de comparer immédiatement l'immatriculation au fichier des véhicules volés ou signalés.

Le programme est en cours d'expérimentation, depuis un peu moins d'un an. Plus d'1,2 million de plaques ont été lues et comparées au fichier des véhicules volés, 65 véhicules mis sous surveillance ont été détectés et 76 interpellations effectuées et la ministre a voulu que ce programme soit généralisé sur l'ensemble du territoire.

Un programme d'extension du dispositif « LAPI », commun à la Police, à la Gendarmerie et aux Douanes a été lancé le 6 décembre 2007.

Le bilan de l'application de la loi de 2006 est donc satisfaisant, mais la menace oblige à aller plus loin dans la lutte contre le terrorisme. Un large plan de protection et d'action antiterroriste, à la fois global, efficace et coordonné, doit ainsi être mis en place.

Tout d'abord, le plan doit être global car protéger contre le terrorisme suppose de protéger contre tout risque d'attentat non seulement les personnes mais également tous les intérêts fondamentaux de la Nation, y compris le patrimoine économique et scientifique. Il ne faut pas oublier – d'ailleurs Al Qaida le dit très explicitement – que le but des terroristes est d'ébranler le système occidental. Les actions peuvent donc prendre des formes multiples, jusqu'à l'utilisation de découvertes par des laboratoires de haute technologie ou de recherche sur les virus, ou la neutralisation de données relatives à la communication ou à l'énergie indispensables à la nation.

Ensuite, l'action doit être efficace, c'est-à-dire apte à prévenir le danger et surtout les attentats. La réorganisation des services de renseignement, récemment engagée, est nécessaire à la pleine efficacité de ces instruments.

Enfin, l'action doit être coordonnée. Le terrorisme est, par définition, transnational. Un pays ne peut s'en protéger seul. C'est pourquoi il faut un développement de la coopération internationale dense et opérationnelle. Ce sera l'un des thèmes de la présidence française de l'Union européenne.

Tels sont les éléments de réponse qui peuvent être apportés aux questions des rapporteurs, étant précisé que l'arrêté qui fixe les tarifs des réquisitions administratives – lesquels seront identiques aux tarifs judiciaires – sera prochainement publié. Un groupe de travail, piloté par la Chancellerie et auquel la ministre de l'intérieur participe, recherche les évolutions nécessaires tout en simplifiant les règles de transmission des réponses.

**M. Éric Diard,** *rapporteur,* s'est déclaré particulièrement satisfait de la prolongation pour quatre ans des dispositions des articles 3, 6 et 9 de la loi.

Il a souhaité que les préfets soient incités à imposer l'installation de vidéosurveillance mais attire l'attention de Mme la ministre sur l'existence d'un flou concernant son financement.

Il s'est réjouit de l'obligation faite aux cybercafés de conserver les données de trafic. Il est, en effet, avéré que le terroriste surnommé *shoe bomber* a utilisé Internet dans un cybercafé avant d'essayer de commettre son attentat sur un vol entre Paris et Miami. C'est un moyen d'accès à Internet plus anonyme qu'une connexion Internet personnelle.

Il a précisé qu'en région PACA, la vidéoprotection a permis de faire baisser notablement la délinquance et d'élucider de nombreuses affaires.

**M. Julien Dray,** *co-rapporteur*, s'est proposé d'offrir aux membres de la commission l'étude évaluative réalisée sur la vidéosurveillance par l'IAURIF, l'Institut d'aménagement et d'urbanisme de la région d'Île-de-France. Il a indiqué ne pas croire que la vidéosurveillance ait fait baisser les chiffres de la délinquance. Elle est certes utile mais il faut savoir l'utiliser. Or le tout-vidéosurveillance est une fuite en avant qui, souvent, dispense du travail de terrain nécessaire.

En réponse à M. Éric Diard, rapporteur, **la ministre** a précisé que, si les préfets sont chargés d'inciter à l'installation de vidéosurveillance, ils ont également pour tâche de mettre en relation l'ensemble des partenaires concernés. Le Gouvernement apporte une aide en la matière, notamment avec le fonds interministériel de prévention de la délinquance.

Les cybercafés comme les points d'accès wi-fi sont des lieux importants qui méritent d'être surveillés de près.

En réponse à M. Julien Dray, co-rapporteur, **la ministre** a précisé que la ville de Saint-Jean-de-Luz n'étant pas équipée de vidéosurveillance, elle n'avait pu directement constater son efficacité, mais qu'elle se fondait sur l'analyse et aux témoignages des maires qui sont les mieux à même de savoir ce qui se passe sur leur territoire. Des maires de Seine-Saint-Denis, dont la plupart sont des amis politiques de M. Dray, lui ont dit que la diminution de la délinquance grâce à la vidéosurveillance allait jusqu'à 100 % sur les parkings et 40 % dans les autres zones.

**M. Michel Hunault** s'est félicité de cette réunion consacrée à l'examen de l'application de la loi du 23 janvier 2006 qui traite d'un sujet difficile, à savoir l'adaptation du dispositif de lutte contre le terrorisme. Il s'est réjoui que la ministre ait rappelé l'exigence que la lutte contre le terrorisme se déroule dans le strict respect de la légalité et des libertés publiques, équilibre qui n'est pas toujours facile à maintenir.

Il a rappelé que la loi de 2006 comporte un dispositif relatif à l'extension du délit de non-justification de ressources, qui concerne le financement même du terrorisme. Or, si la loi de 1996 contre le blanchiment de l'argent a été votée en application d'une convention de 1990 du Conseil de l'Europe, qui a été réactualisée en 2002, la France n'a toujours pas transposé la troisième directive de l'Union européenne de 2005 ni ratifié la convention du Conseil de l'Europe de 2005 contre le blanchiment et le financement du terrorisme. Quand va-t-elle y procéder ?

Enfin, un débat difficile a eu lieu à l'assemblée parlementaire du Conseil de l'Europe lors de la dernière session, il y a dix jours, sur l'établissement d'une liste noire des organisations terroristes. Quelle suite le Gouvernement entend-il donner à la recommandation du Conseil de l'Europe à ce sujet, sachant que la liste concerne certaines organisations situées en France ?

**M. Philippe Goujon** s'est félicité également de cette réunion consacrée à l'examen de la loi du 23 janvier 2006. Nul ne doute aujourd'hui que la France soit dotée d'un dispositif efficace de prévention du terrorisme – rendu encore plus performant par la loi de 2006 – , et respectueux des droits fondamentaux.

Le régime juridique de la vidéosurveillance, aujourd'hui modernisé et adapté, concilie bien la défense des libertés et la prévention du terrorisme. Estimant que la préconisation du rapport tendant à ce que les préfets imposent la vidéosurveillance aux gestionnaires d'équipements confrontés à des risques terroristes doit être approuvée, il s'est déclare étonné de la réaction de M. Dray, avec lequel il a travaillé sur ces sujets à la région, et qui n'a pas hésité à recourir à des dispositifs de vidéoprotection, notamment dans les transports. D'ailleurs, le président de la région Île-de-France s'est déclaré très favorable à leur développement. Quant à l'étude de l'IAURIF, examinée par l'Observatoire national de la délinquance, c'est la mauvaise exploitation de la vidéoprotection – qui est de la responsabilité de ses utilisateurs – qu'elle met en cause.

Il est donc indispensable que le système de vidéosurveillance retenu soit bien adapté et que les personnels qui l'utilisent soient formés en conséquence. Près de 300 villes en France en sont équipées et la baisse de la délinquance constatée montre qu'elle a eu un incontestable impact, même si elle n'en constitue pas le seul facteur. Personne n'a jamais prétendu que ce type de dispositif était destiné à remplacer toute forme de protection humaine. Mais, dans les zones sensibles, les lieux de forte fréquentation ou de grands rassemblements comme les abords des gares et les lieux touristiques, il a démontré son utilité aussi bien pour le contrôle de la délinquance que pour la lutte antiterroriste. Il est également efficace dans les transports en sous-sol. Si le SRPT – le service régional de la police des transports – a enregistré une baisse de près de 12 % de la délinquance en 2007 dans le réseau souterrain d'Île-de-France, c'est en grande partie grâce à lui. Le week-end dernier, un SDF est malheureusement décédé en tombant sur la voie d'une station de métro parisien. C'est grâce aux caméras installées sur le quai

que la police a pu identifier les conditions dans lesquelles s'était produit cet évènement.

Rappelant qu'à Londres, ce sont quelque 65 000 caméras qui sont reliées à Scotland Yard alors qu'à Paris, il n'y en a aucune qui le soit pour des raisons de sécurité, M. Philippe Goujon a demandé où en était le développement de la vidéoprotection dans la capitale et quelle était la contribution de la mairie de Paris en la matière.

**M. Jacques Alain Bénisti** a reconnu l'intérêt de la vidéosurveillance mais met en garde contre la tentation d'en faire une panacée. Il a considéré qu'elle n'est qu'un des éléments de la prévention de la délinquance parmi tous ceux prévus, par exemple, dans la loi relative à la prévention de la délinquance.

Il a fait ensuite observer que placer des dispositifs de vidéosurveillance dans les cités sensibles, par exemple, est d'une utilité limitée car la plupart des faits délictueux ont lieu à l'extérieur, notamment en centre ville.

Cela étant, et même s'il n'est pas possible, faute de recul, d'établir un constat définitif, les résultats de la vidéosurveillance sont très concluants. Ainsi, les quatre caméras installées dans la ville dont M. Bénisti est le maire ont permis d'arrêter une dizaine de délinquants qu'il aurait été impossible de prendre sur le fait sans ce dispositif.

Trois avantages peuvent être retirés des installations de vidéosurveillance.

Le premier est la rapidité d'intervention des forces de police, puisque celle-ci peut être immédiatement alertée lorsque les images font l'objet d'un visionnage en direct.

Le deuxième avantage est l'aide considérable apportée à l'élucidation des actes délictueux, même lorsque le dispositif se borne à un enregistrement d'images dont le visionnage est différé.

Le troisième avantage est le sentiment de sécurité ressenti par les citoyens dans les zones surveillées par des caméras.

Les seuls mécontents sont donc les délinquants qui se trouvent démunis face à cette nouvelle forme d'élucidation des affaires par vidéo.

En réponse, **la ministre** a apporté les précisions suivantes :

— Les textes mentionnés par M. Hunault relèvent de la Chancellerie et non du ministère de l'intérieur, qui ne peut donc donner aucune information les concernant.

— La « liste noire » liée au terrorisme fait l'objet de nombreuses contestations car elle a été élaborée par les États-unis – y figurer entraîne l'interdiction de s'y rendre – et est extrêmement large.

Cette liste, en elle-même, ne donne pas lieu à l'application de mesures particulières par la France. Néanmoins, il est évident que les services de sécurité suivent les personnes qui peuvent présenter un danger, utilisant également pour cela le système des visas délivrés par nos consulats dans les pays à risque. Ce qui est important, c'est de contrôler les personnes en fonction de leur dangerosité potentielle plutôt que de leur appartenance à une structure, surtout si cette dernière n'a pas d'implantation en France.

— Pour que la vidéoprotection soit efficace, il faut qu'elle soit d'une certaine qualité. C'est pourquoi l'effort doit porter non seulement sur le nombre de caméras mais aussi sur la qualité de l'image. Dans le cas de l'accident dramatique dont a été victime cet été un journaliste italien, le film tiré du système de vidéosurveillance était inexploitable du fait de la vétusté des caméras et il n'a pas permis de retrouver les coupables.

Le développement de la vidéoprotection – auquel la ministre s'est déclarée attachée et pour lequel elle a mis des structures en place – doit impérativement s'effectuer dans le respect des libertés publiques et individuelles. Les groupes terroristes n'attendent que le moment où les gouvernements porteront atteinte aux droits individuels, et il faut veiller à ce que la recherche de protection ne se retourne pas contre les peuples, comme la ministre a eu l'occasion de l'affirmer à plusieurs reprises à des chefs d'État ou de gouvernement étrangers.

— Au-delà du triplement du nombre de caméras prévu sur l'ensemble de la France, il est envisagé à Paris un « plan 1000 » : la préfecture de police – donc le ministère de l'intérieur – installera sur la voie publique mille caméras, soit un peu plus de trois fois le dispositif existant accessible aux services de sécurité. Pour y parvenir, un partenariat public-privé sera mis en place. Cela s'ajoutera aux efforts particuliers qui sont faits notamment par la RATP et la SNCF. Parallèlement, il est prévu d'ouvrir aux services de sécurité l'accès à 150 caméras privées implantées sur un certain nombre de lieux stratégiques.

— Il n'est, bien entendu, pas question que la vidéosurveillance remplace les autres moyens de protection contre le terrorisme. C'est un moyen supplémentaire, qui s'ajoute au renseignement – élément fondamental puisqu'il permet de repousser les risques – et au contrôle aux frontières – qui suppose des croisements de fichiers et une présence humaine très importante. Si la vidéoprotection est une aide à la réactivité en même temps qu'un élément de dissuasion, il est évident qu'elle ne remplace en rien une présence sur le terrain, que la ministre s'emploie également à renforcer comme le montre le plan qu'elle a développé en Seine-Saint-Denis et qui a vocation à être élargi à d'autres départements.

*La Commission a autorisé le dépôt du rapport en vue de sa publication.*

# SUIVI DES TEXTES D'APPLICATION DE LA LOI N° 2006-1964 DU 23 JANVIER 2006 RELATIVE À LA LUTTE CONTRE LE TERRORISME ET PORTANT DISPOSITIONS DIVERSES RELATIVES À LA SÉCURITÉ ET AUX CONTRÔLES FRONTALIERS

| Article de la loi | Base légale | Nature du texte | État d'avancement | Objet |
|---|---|---|---|---|
| Article 1 et 2 | Art. 10 et 10-1 de la loi n° 95-73 du 21 janvier 1995 | Décret en Conseil d'État | Décret n° 2006-929 du 28 juillet 2006 | Modalités d'application des dispositions relatives à la vidéosurveillance |
| Article 1 et 2 | Art. 10 et 10-1 de la loi n° 95-73 du 21 janvier 1995 | Arrêté ministériel | Arrêtés du ministre de l'intérieur du 26 septembre 2006 et du 3 août 2007 | Définition des normes techniques des dispositifs de vidéosurveillance |
| Article 3 | Art 78-2 du code de procédure pénale | Arrêté ministériel | Arrêté conjoint du ministre de l'intérieur et du ministre de la justice du 26 avril 2006 | Désignation des arrêts sur les liaisons ferroviaires internationales pouvant donner lieu à application de l'article 78-2 du CPP |
| Article 4 | Art. 25 de la loi n° 95-73 du 21 janvier 1995 | Arrêté ministériel | Arrêté du ministre de l'intérieur du 23 octobre 2006 | Normes techniques applicables aux matériels d'immobilisation des véhicules |
| Article 5 | Art. L. 34-1 du code des postes et des communications électroniques | Dispositions d'application directe | | Obligation de conservation des données de connexion par les personnes fournissant au public une connexion Internet |
| Article 6-I | Art. L. 34-1-1 du code des postes et des communications électroniques | Décret en Conseil d'État, après avis CNIL (28 sept. 2006) et avis CNIS (12 juillet 2006) | Décret n° 2006-1651 du 22 décembre 2006 : il renvoie certaines modalités d'application à des arrêtés (en attente) | Modalités d'application de la procédure de réquisition administrative des données conservées par les opérateurs de télécommunication |
| Article 6-I | Art. L. 34-1-1 du code des postes et des communications électroniques | Décision de la CNCIS sur proposition du ministre de l'intérieur | Décisions n° 1-2006 et n° 1-2007 de la CNCIS | Désignation de la personnalité qualifiée et de ses adjoints |
| Article 6-II | Art 6 de la loi n° 2004-575 du 21 juin 2004 | Décret en Conseil d'État après avis CNIL (20 décembre 2007) | **Décret en attente** | Modalités d'application de la procédure de réquisition administrative des données conservées par les hébergeurs de site Internet |
| Article 6-III | Loi n° 91-646 du 10 juillet 1991 | Dispositions d'application directe | | Prérogatives de la CNCIS |

| Article de la loi | Base légale | Nature du texte | État d'avancement | Objet |
|---|---|---|---|---|
| Article 7- I et II | Dispositions non codifiées | Arrêté après avis CNIL (14 septembre 2006) | Arrêté du ministre de l'Intérieur et du ministre de l'économie et des finances du 3 novembre 2006 | Modernisation du Fichier national transfrontière |
| Article 7- I et II | Dispositions non codifiées | Arrêté après avis CNIL (14 septembre 2006) | Arrêté du ministre de l'Intérieur, du ministre de la défense et du ministre des transports du 19 décembre 2006 | Création d'un traitement automatisée des données relatives aux passagers des compagnies aériennes |
| Article 7- IV | Dispositions non codifiées | Décret en Conseil d'État après avis CNIL (14 septembre 2006) | Décret n° 2006-1630 du 19 décembre 2006 | Modalités de transmission des données relatives aux passagers par les compagnies aériennes |
| Article 7-V | Dispositions non codifiées | Décret en Conseil d'État | Décret n° 2006-725 du 22 juin 2006 | Conditions de mise en œuvre des sanctions prévues en cas de méconnaissance de leurs obligations par les compagnies aériennes |
| Article 8 | Art. 26 de la loi n° 2003-239 du 18 mars 2003 | Arrêté après avis de la CNIL (8 février 2007) | Arrêté du ministre de l'Intérieur, du ministre de la défense et du ministre des transports du 2 mars 2007 | Mise en œuvre expérimentale du dispositif de lecture automatisée des plaques d'immatriculation |
| Article 9 | Dispositions non codifiées | Décret en Conseil d'État après avis CNIL (5 oct. 2006 pour n° 2007-86 et n° 2007-391 ; 18 jan. 2007 pour n° 2007-1136) sauf D n° 2007-87 (décret simple) | Décret n° 2007-86 du 23 janvier 2007, décret n° 2007-87 du 23 janvier 2007, décret n° 2007-391 du 21 mars 2007, décret n° 2007-1136 du 25 juillet 2007 | Accès direct des agents des services chargés de la lutte contre le terrorisme à différents fichiers tenus par le ministère de l'intérieur |
| Article 9 | Dispositions non codifiées | Arrêté du ministre de l'intérieur et du ministre de la défense | Arrêté du ministre de l'intérieur et du ministre de la défense du 27 juin 2006 | Désignation des services de renseignement du ministère de la défense pouvant accéder aux fichiers tenus par le ministère de l'intérieur |
| Article 10 | Art. 23 de la loi n° 2003-239 du 18 mars 2003 | Arrêté | Arrêté du ministre de l'intérieur, du ministre de la justice, du ministre de la défense et du ministre du budget du 12 juillet 2007 | Mesures inscrites dans le fichier des personnes recherchées |
| Article 11 | Art. 421-6 du code pénal | Dispositions d'application directe | | Criminalisation de l'association de malfaiteurs terroriste |

| Article de la loi | Base légale | Nature du texte | État d'avancement | Objet |
|---|---|---|---|---|
| Article 12 | Art. 706-24 du code de procédure pénale | Décret en Conseil d'État en tant que de besoin | Art 13 du décret n° 2007-1388 du 26 septembre 2007 | Identification par leur numéro d'immatriculation administrative des officiers et agents de police judiciaire chargés de la lutte contre le terrorisme |
| Article 13 | Art. 30 de la loi n° 78-17 du 6 janvier 1978 | Décret en Conseil d'État après avis CNIL (11 janvier 207) | Décret n° 2007-451 du 25 mars 2007 et Décret n° 2007-914 du 15 mai 2007 | Traitements automatisés intéressant la sûreté de l'État, la défense ou la sécurité publique |
| Article 14 | Art. 706-22-1 du code de procédure pénale | Dispositions d'application directe | | Centralisation de l'application des peines en matière terroriste |
| Article 15 | Art. 706-25 du code de procédure pénale | Dispositions d'application directe | | Jugement des mineurs terroristes par des cours d'assises spécialement composées |
| Article 16 | Art. 16 et 20 du code de procédure pénale | Décret en Conseil d'État | Décret n° 2006-1329 du 31 octobre 2006 | Désignation des officiers de police judiciaire de la police nationale |
| Article 17 | Art. 706-88 du code de procédure pénale | Dispositions d'application directe | | Prolongation de la durée de la garde à vue en matière de terrorisme |
| Article 18 | Art. 800 du code de procédure pénale | Décret en Conseil d'État + arrêté du ministre de l'économie et des finances et du garde des sceaux | Décret n° 2006-358 du 24 mars 2006 et arrêté du ministre de la justice et du ministre de l'économie et des finances du 22 août 2006 | Modalités de remboursement des réquisitions adressées aux opérateurs de télécommunications |
| Article 20 | Art. L. 126-1 du code des assurances | Dispositions d'application directe | | Extension de l'indemnisation des victimes d'actes de terrorisme à leurs ayants droit |
| Article 21 | Art. 25-1 du code civil | Dispositions d'application directe | | Extension des possibilités de déchéance de la nationalité |
| Article 22 | Loi n° 86-1067 du 30 septembre 1986 | Dispositions d'application directe | | Suppression du conventionnement des chaînes de télévision extra-communautaires |
| Article 23 | Art. L. 564-1 à L. 564-6 du code monétaire et financier | Décret en Conseil d'État | Décret n° 2007-545 du 11 avril 2007 | Gel administratif des avoirs des terroristes |
| Article 24 | Art. 321-6 et 321-10-1 du code pénal, art 706-73 du code de procédure pénal | Dispositions d'application directe | | Délit de non justification de ressources |

| Article de la loi | Base légale | Nature du texte | État d'avancement | Objet |
|---|---|---|---|---|
| Article 25 | Loi n° 83-629 du 12 juillet 1983 | Dispositions d'application directe | | Agrément des agents de sécurité privée |
| Article 26 | Art. L. 213-5 et L. 321-8 du code de l'aviation civile | Décret en Conseil d'État | Décret n° 2007-775 du 9 mai 2007 | Accès aux zones réservées des aéroports |
| Article 27 | Art. 31 de la loi n° 95-73 du 21 janvier 1995 | Dispositions d'application directe | | Application outre-mer des dispositions relatives à la vidéosurveillance |
| Article 28 | | Dispositions d'application directe | | Application de la loi outre-mer |
| Article 29 | Art. L. 126-2 et L. 126-3 du code des assurances | Décret en Conseil d'État | Décret n° 2006-1202 du 29 septembre 2006 | Dérogations et exclusions applicables aux contrats d'assurance en matière de terrorisme |
| Article 30 | Art. 39 sexies de la loi du 29 juillet 1981 | Dispositions d'application directe | | Diffamation des personnels du ministère de la défense |
| Article 31 | Art. 42-12 de la loi n° 84-610 du 16 juillet 1984 | Décret en Conseil d'État | Décret n° 2006-388 du 15 mars 2006 | Interdiction administrative de stade |
| Article 32 | Dispositions non codifiées | Dispositions d'application directe | | Application de la loi |
| Article 33 | Dispositions non codifiées | Arrêté interministériel | Arrêté du ministre de l'intérieur, du ministre de la justice, du ministre de la défense et du ministre de l'outre-mer du 31 mars 2006 | Désignation des services de police et de gendarmerie spécialement chargés de la prévention et de la répression des actes de terrorisme |

# CIRCULAIRES D'APPLICATION DE LA LOI N° 2006-1964 DU 23 JANVIER 2006 RELATIVE À LA LUTTE CONTRE LE TERRORISME ET PORTANT DISPOSITIONS DIVERSES RELATIVES À LA SÉCURITÉ ET AUX CONTRÔLES FRONTALIERS

— Circulaire du garde des sceaux, ministre de la justice du 3 février 2006 relative à la loi n° 2006-1964 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

— Circulaire du ministre d'État, ministre de l'intérieur et de l'aménagement du territoire du 21 juillet 2006 relative à l'application de la loi n° 2006-1964 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

— Circulaire du ministre d'État, ministre de l'intérieur et de l'aménagement du territoire du 29 août 2006 relative à l'application du dispositif des interdictions administratives de stade créé par l'article 31 de la loi n° 2006-1964 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

— Circulaire du ministre d'État, ministre de l'intérieur et de l'aménagement du territoire du 26 octobre 2006 relative à l'application des articles 10 et 10-1 de la loi n° 95-73 du 21 janvier 1995 modifiée d'orientation et de programmation relative à la sécurité.

# PERSONNES AUDITIONNÉES

- **Ministère de l'intérieur, de l'outre-mer et des collectivités territoriales**

  **Direction générale de la police nationale (DGPN)**

  — M. Bernard SQUARCINI, directeur de la surveillance du territoire (DST)

  — M. Jean-Yves TAUPIN, directeur central de la police aux frontières (DCPAF)

  — M. Christophe CHABOUD, chef de l'Unité de coordination de la lutte antiterroriste (UCLAT)

  **Direction des libertés publiques et des affaires juridiques (DLPAJ)**

  — M. Laurent TOUVET, directeur

  **Personnalité qualifiée au sens de l'article L. 34-1-1 du code des postes et des communications électroniques**

  — M. François JASPART, inspecteur général de la police nationale, personnalité qualifiée

- **Ministère de la justice**

  **Direction des affaires criminelles et des grâces (DACG)**

  — M. Jean-Marie HUET, directeur

  **Tribunal de grande instance de Paris**

  — Mme Anne KOSTOMAROFF, vice-procureur, chef de la section antiterroriste au parquet

- **Commission nationale de l'informatique et des libertés (CNIL)**

  — M. François GIQUEL, vice-président

  — Mme Sophie TAVERNIER, directrice des affaires juridiques

- **Commission nationale de contrôle des interceptions de sécurité (CNCIS)**

  — M. Jean-Louis DEWOST, président

  — M. Rémi RECIO, délégué général

  — M. François COUDERT, chargé de mission

- **Association française des opérateurs mobiles (AFOM)**

  — M. Jean-Marie DANJOU, délégué général

  — MM. Jean-Pierre COUSTEL et Richard KASTELER (ORANGE)

  — M. Nicolas HELLÉ (SFR)

  — M. Gilles CAMPAGNAC (BOUYGUES TELECOM)

- **Association française des fournisseurs d'accès (AFA)**

  — Daniel FAVA, président, directeur Business et qualité de Télécom Italia Alice