

RDTIC

REVUE DE DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION

La revue de droit des techniques de l'information et de la communication (RDTIC) est un service proposé par DROIT-TIC - www.DROIT-TIC.com.

Elle vous propose une synthèse non exhaustive des informations juridiques mise en ligne sur le site DROIT-TIC durant le mois écoulé. Vous y trouverez non seulement des articles (actualités, analyses, synthèses, doctrines...), mais encore des décisions de justice, la doctrine de certaines autorités administratives indépendantes et des textes normatifs.

Conseil scientifique

- Julien Le Clainche, chercheur
- François-Xavier Boulouin, avocat BCTG Associés
- Anthony Grevin, juriste M6 Web
- Vincent Duseauguey, juriste M6 Web
- Julien Linsolas, juriste Cap Gemini
- Olivier Gnos, architecte logiciel
- Marie-Alix Boussard, allocataire de recherche
- Franck Macrez, ERCIM UMR 5815 Université Montpellier I

Informations légales

La RDTIC est protégée par les normes nationales et internationales en vigueur, notamment celles relatives à la propriété intellectuelle.

Citation : RDTIC n° XX, mois année, DROIT-TIC, p. XX.

Les articles sont la propriété de leurs auteurs. Si vous souhaitez les contacter, rendez-vous sur le site DROIT-TIC.com, rubrique "DROIT-TIC et vous", "L'équipe de DROIT-TIC".

La lecture de la RDTIC emporte le respect des conditions d'utilisation du site DROIT-TIC qui sont disponibles à l'adresse : <http://www.droit-tic.com/index2.php?page=conditions.php>

Vous pouvez présenter vos observations, remarques, soutiens, encouragements et autres critiques constructives en écrivant à julien@droit-ntic.com.

DROIT-TIC / Julien Le Clainche, 5 rue des chênes verts, 34110 MIREVAL.

ANALYSES / ACTUALITÉS

■ **RECOMMANDATION DE LA CNIL SUR LES SITES WEB DES PARTICULIERS**

Par M. Vincent DOMNESQUE, Juriste TIC - BRM Avocats

■ **LE WHOIS DU .EU MIS EN ATTENTE**

M. Jean-François Poussard, Rédacteur en Chef MailClub.info

■ **L'OBLIGATION POUR LES FAI DE METTRE À DISPOSITION DES LOGICIELS DE CONTRÔLE PARENTAL p. 19**

Par M. Vincent DOMNESQUE, Juriste TIC - BRM Avocats.

FOCUS

■ **LA NAISSANCE D'UN DOUBLE RÉGIME D'ACCES AUX DONNÉES RELATIVES AU TRAFIC**

Par M. Julien LE CLAINCHE, Chercheur, directeur de DROIT-TIC

■ **DÉCISION N° 2005-532 DC DU 19 JANVIER 2006 LOI RELATIVE À LA LUTTE CONTRE LE TERRORISME ET PORTANT DISPOSITIONS DIVERSES RELATIVES À LA SÉCURITÉ ET AUX CONTRÔLES FRONTALIERS**

■ **LOI N° 2006-64 DU 23 JANVIER 2006 RELATIVE A LA LUTTE CONTRE LE TERRORISME ET PORTANT DISPOSITIONS DIVERSES RELATIVES A LA SECURITE ET AUX CONTRÔLES FRONTALIERS**

TEXTES OFFICIELS

■ **Décret N° 2006-6 DU 4 JANVIER 2006 RELATIF À L'HEBERGEMENT DES DONNEES DE SANTE À CARACTERE PERSONNEL ET MODIFIANT LE CODE DE LA SANTE PUBLIQUE**

JURISPRUDENCES

■ **TGI VANNES, 13 juillet 2005, UNIVERSITÉ DE BRETAGNE SUD / M. A ET ALII**

INFORMATIQUE ET LIBERTÉS, VIE PRIVÉE



FOCUS SUR :

LA LOI N° 2004-66 DU 23 JANVIER 2006 RELATIVE A LA LUTTE CONTRE LE TERRORISME ET PORTANT DISPOSITIONS DIVERSES RELATIVES A LA SECURITE ET AUX CONTROLES FRONTALIERS

- LA NAISSANCE D'UN DOUBLE RÉGIME D'ACCES AUX DONNÉES RELATIVES AU TRAFIC

 - DÉCISION N° 2005-532 DC DU 19 JANVIER 2006 LOI RELATIVE À LA LUTTE CONTRE LE TERRORISME ET PORTANT DISPOSITIONS DIVERSES RELATIVES À LA SÉCURITÉ ET AUX CONTROLES FRONTALIERS

 - 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
-

LA NAISSANCE D'UN DOUBLE RÉGIME D'ACCÈS AUX DONNÉES RELATIVES AU TRAFIC

Par M. JULIEN LE CLAINCHE,
Chercheur
Directeur de DROIT-TIC

Le 19 janvier 2006, le Conseil Constitutionnel a été amené à se prononcer sur la conformité de la loi n° 2006-64 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers¹.

En effet, plus de soixante députés ont remis en question la constitutionnalité, non seulement des dispositions relatives à la conservation des données relatives au trafic et de localisation, mais encore celles se rapportant aux dispositifs de contrôle des données signalétiques des véhicules ou encore à la représentation syndicale au sein des instances paritaires. Plus généralement, c'était le principe de clarté et d'intelligibilité de la loi, qui était remis en cause². Essayons de mesurer la portée de cette décision n° 2005/532 DC du 19 janvier 2006³ sur le régime applicable aux données relatives au trafic, les autres aspects étant provisoirement laissés de côté.

Les données relatives au trafic sont celles qui sont traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation⁴. Leur conservation a fait l'objet d'une

¹ 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, J.O n° 20 du 24 janvier 2006 page 1129, texte n° 1.

<http://www.legifrance.gouv.fr/texteconsolide/PPEFF.htm>, document consulté le 29 janvier 2006.

² Pour plus d'informations se reporter au texte de la saisine du Conseil Constitutionnel, Décision n° 2005-532 DC - 19 janvier 2006, Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, SAISINE du Conseil constitutionnel par plus de soixante sénateurs.

<http://www.conseil-constitutionnel.fr/decision/2006/2005532/saisine1.htm>, document consulté le 29 janvier 2006.

³ Décision n° 2005-532 DC - 19 janvier 2006, Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

http://droit-tic.com/juris/aff.php?id_juris=63, également disponible sur le site du Conseil Constitutionnel <http://www.conseil-constitutionnel.fr/decision/2006/2005532/2005532dc.htm>,

documents consultés le 29 janvier 2006.

⁴ Code des postes et communications électroniques, article L.32 18°. Directive 2002/58 CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des

régulation aux contours encore flous et indistincts⁵, dont l'association « Imaginons un Réseau Internet Solidaire » a dressé la chronologie⁶. La finalité de cette conservation est de permettre aux autorités de pouvoir retrouver les auteurs d'infractions, délits et crimes commis par le biais des réseaux informatiques. Notons d'emblée que le caractère proportionné et l'efficacité de cette conservation peuvent être débattus⁷, et le sont, notamment au niveau communautaire⁸. La loi n° 2006-64 est venue modifier le régime institué par la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne⁹. En effet, la loi nouvelle étend la liste des informations qui doivent être conservées, celle des personnes débitrices de cette obligation, la durée de conservation. Enfin, les nouvelles dispositions assouplissent les conditions d'accès aux données.

Quelles données doivent être conservées ? Qui doit les contrôler ?

L'article L. 34-1 du Code des postes et des communications électroniques (CPCE) pose le principe de l'effacement des données relatives au trafic avant d'énumérer les exceptions dont il peut souffrir. Les informations d'identification exigées par l'architecture des réseaux de communications constituent la base des

communications électroniques, JOCE du 23 Novembre 1995 n° L. 281 p. 31. Article 2. b).

⁵ Pour des analyses récentes du cadre juridique applicable aux données relatives au trafic voir, MATHIAS G. et LORRAIN A-C, « Données de connexion : un état des lieux ou une première tentative de démêlage de la toile législative », RLDI 2005/11, n° 334, p. 48. Voir également, REYNAUD, P. « Le fournisseur d'accès et la conservation des données engendrées par les communications électroniques », Com. Com. Electr. N° 6, juin 2005, Etd. n° 23. Pour des ressources en ligne voir, LE CLAINCHE, J. « Toujours pas de consensus sur la rétention des données relatives au trafic », DROIT-TIC, 24 octobre 2005 in RDTIC n° 46, p. 4. Voir également, 2005 et à LE CLAINCHE, J., « Désaccord entre le Conseil et la Commission sur la durée de conservation des données de trafic », DROIT-TIC, 3 octobre 2005 in RDTIC n° 46, p. 11. et LE CLAINCHE, J., « Vers une durée de rétention sans... retenue ? », DROIT-TIC, 18 juillet 2005, in RDTIC n° 43, p. 2.

⁶ Imaginons un Réseau Internet Solidaire (I.R.I.S.), « Rétention des données de trafic dans les communications électroniques, suivi des mesures françaises et européennes et de la plainte d'IRIS contre la France auprès de la CE (LSQ) », document consulté le 29 janvier 2006.

⁷ Sur ce point voir, LE CLAINCHE J. ., « Désaccord entre le Conseil et la Commission sur la durée de conservation des données de trafic », précité : « si une requête dans ce type de traitement peut mettre entre cinquante et cent ans pour aboutir, il est probable que le système de conservation des données de trafic ne comble pas toutes les attentes qui sont placées en lui ».

⁸ Sur ce point voir, NUNO ALVARO, N., rapport 2004/0813(CNS) au Parlement européen pour la commission des libertés, de la justice et des affaires intérieures, p. 6.

⁹ La loi n° 2006-64 est venue modifier le régime institué par la loi n° 2001/1062 du 15 novembre 2001 relative à la sécurité quotidienne, J.O n° 266 du 16 novembre 2001 page 18215.

données qui permettent la surveillance des transactions électroniques. Il s'agit, au terme de l'article 6 de la loi nouvelle, des « *données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* ». Concrètement sur Internet, il peut s'agir des adresses « IP » auxquelles sont associées la date et l'heure de la connexion, le type d'usage (courriel, transfert de fichiers ou Web) et des requêtes ou du message. Dans le cadre d'un réseau téléphonique, il pourra notamment s'agir des numéros appelants et appelés, de la date et de la durée de la communication, de l'identifiant du terminal. Notons que la liste des données ne semble pas limitative et qu'il faudra attendre l'adoption du décret d'application pour en connaître la teneur précise. D'une part, il s'agit pour les débiteurs de l'obligation de conservation d'être en mesure de savoir précisément à quoi ils sont tenus. D'autre part, une liste concurrente est actuellement débattue au niveau communautaire, et il serait dommageable que l'obligation de conservation des données techniques française soit plus large que celle qui sera prévue par la directive en cours de discussion. Notons également qu'il ne s'agit pas, en principe, de traiter le contenu des communications mais seulement les informations qui y sont relatives¹⁰.

Pourtant, la loi nouvelle soumet l'accès à ces données au contrôle de la Commission Nationale de Contrôle des Interceptions de sécurité (CNCIS)¹¹ : « *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* »¹². Cette compétence de la CNCIS est surprenante dans la mesure où, d'après le texte, il ne s'agit pas d'intercepter les communications, mais seulement de conserver certaines informations à leur sujet. Cette compétence étonnante conduit à deux alternatives. Soit la finalité du traitement n'est pas clairement définie et pourra évoluer vers la conservation du contenu des communications. Soit il s'agit de retirer la compétence, pourtant légitime, de la Commission Nationale de l'Informatique et des Libertés (CNIL), institution dont l'indépendance est indiscutée et qui avait émis de *nombreuses réserves*

¹⁰ Loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, J.O n° 177 du 2 août 2000 page 11903. Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques. Loi 2003-239 du 18 mars 2003 pour la sécurité intérieure, J.O n°66 mars 2003, p.4761

¹¹ La CNCIS a été instituée par l'article 13 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

¹² Article 6 de la loi n° 2006-64 du 23 janvier 2006.

quant au projet de loi relatif à la lutte contre le terrorisme¹³. En effet, si les deux commissions sont des autorités administratives indépendantes, force est de constater que les pouvoirs de la CNIL¹⁴ sont bien plus étendus que ceux de la CNCIS, dont les membres sont moins nombreux et présentent peut-être moins de garanties d'indépendance. En effet, celle-ci ne dispose que d'un pouvoir de recommandations au ministre de l'intérieur lorsqu'elle constate « *un manquement aux règles édictées par le présent article ou une atteinte aux droits et libertés* »¹⁵.

Quelles personnes doivent conserver les données relatives au trafic ?

Le texte nouveau inséré à l'article L. 34-1 I du CPCE soumet aux dispositions de la loi n° 2006-64 « *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* ». Comme le note le Forum des Droits sur l'Internet, la disposition vise tout particulièrement les « *Cybercafés* »¹⁶ en plus des prestataires traditionnels d'accès au réseau. Ainsi, une société commerciale qui propose à ses clients un accès au réseau Internet à titre accessoire, par exemple dans le cadre d'une activité de transport ou de restauration est soumise à l'obligation de conservation. Les prestataires de services à titre gratuit sont également visés par le texte. Il semblerait que ce critère de l'activité professionnelle conduise à soumettre aux dispositions de la loi « *les mairies, bibliothèques et universités si leurs activités les conduisaient à titre accessoire à fournir une prestation identique à celle d'un cybercafé* »¹⁷. En revanche, une association peut-elle être considérée comme conduisant une activité professionnelle ? Faisant écho à la CNIL, il convient de se demander si ce critère n'est pas inadéquat au regard des « *incertitudes qui s'attachent (...) à une telle définition* »¹⁸. Toutefois, il semble assuré que seules sont

¹³ CNIL, délibération n° 2005-208 du 10 octobre 2005 portant avis sur le projet de loi relatif à la lutte contre le terrorisme.

http://www.droit-tic.com/juris/aff.php?id_juris=40, document consulté le 29 janvier 2006.

Voir également, COSTES, L. « *Nombreuses réserves de la CNIL sur le projet de loi relatif à la lutte contre le terrorisme* », RDLI 2005/10, n° 294, p. 34.

¹⁴ Sur les pouvoirs de la CNIL voir, LE CLAINCHE J., « *Pouvoirs a posteriori de la CNIL : les risques de l'excès de prudence* », RDLI 2005/11, n° 333, p. 43.

¹⁵ Nouvel article L. 34-1 CPCE.

¹⁶ Forum des Droits sur l'Internet, « *Conservation des données de connexion – Nouveau régime issu de la loi anti-terrorisme* », 26 janvier 2006.

<http://www.foruminternet.org/actualites/lire.phtml?id=1001>, document consulté le 29 janvier 2006.

¹⁷ Forum des Droits sur l'Internet, « *Conservation des données de connexion – Nouveau régime issu de la loi anti-terrorisme* », 26 janvier 2006, précité.

¹⁸ CNIL, délibération n° 2005-208 du 10 octobre 2005, précitée.

visées les personnes physiques ou morales dont l'activité professionnelle est d'offrir au public à titre accessoire ou principal une connexion au réseau Internet, « *ce qui exclut de cette définition notamment les entreprises ou administrations qui assurent un accès au réseau à leurs seuls salariés ou agents* »¹⁹.

Au niveau communautaire avait été souligné la charge financière que l'obligation de conservation des données relatives au trafic faisait peser sur les acteurs d'un marché sur lequel la concurrence est âpre²⁰. La loi française a donc anticipé le texte de la prochaine directive qui prévoit « *une disposition qui oblige les États membres à dédommager les fournisseurs de communications électroniques des surcoûts supportés en raison de l'obligation de conservation* »²¹. Ainsi, la loi française prévoit-elle que « *les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnés au premier alinéa pour répondre à ces demandes font l'objet d'une compensation financière* »²². Ce dédommagement est d'autant plus nécessaire à la mise en œuvre d'un système proportionné de conservation des données, que les prestataires techniques ne conservent plus systématiquement les données de trafic à des fins de facturation. En effet, le développement des offres forfaitaires de communication et d'offres « illimitées » ne rend plus nécessaire la conservation systématique des informations relatives au trafic.

Vers un double régime des conditions d'ouverture du traitement des données relatives au trafic.

Le projet de loi relative à la lutte contre le terrorisme disposait qu'« *afin de prévenir et de réprimer les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs (...) la communication des données conservées et traitées...* ». Cette disposition devait modifier non seulement l'article L. 34-1 du CPCE, mais encore l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique²³. Comme l'a fait observer la CNIL, « *cette distinction n'est pas neutre dans la mesure où ces dispositions légales doivent, pour chacune d'entre elles, être*

précisées par un décret en Conseil d'Etat pris après avis de la CNIL précisant notamment la nature et la durée de conservation des données devant être conservées, qui peuvent donc être différentes ». La Commission recommandait « *donc l'abandon de la référence à l'article L.34-1 dans la rédaction du premier alinéa de l'article 7 du projet de loi* »²⁴.

Au terme de l'article 66 de la Constitution, « *nul ne peut être arbitrairement détenu. - L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi* ». La répression des infractions, délits et crimes, au nombre desquels sont comptés les actes de terrorismes, est donc une compétence de l'autorité judiciaire constitutionnellement garantie. Or, le projet de loi proposait de permettre l'accès aux données relatives au trafic dans le cadre des pouvoirs de police administrative et judiciaire sans contrôle par des autorités judiciaires²⁵.

Le Conseil Constitutionnel, après avoir fait observé que « *les données techniques (...) peuvent déjà être obtenues, en application des dispositions du code de procédure pénale, dans le cadre d'opérations de police judiciaire destinées à constater les infractions à la loi pénale* »²⁶, considère que « *les réquisitions de données permises par les nouvelles dispositions constituent des mesures de police purement administrative (...) que, dès lors, en indiquant qu'elles visent non seulement à prévenir les actes de terrorisme, mais encore à les réprimer, le législateur a méconnu le principe de la séparation des pouvoirs* ».

Certains auteurs ont conclu à la validation de la loi n° 2006-64²⁷. Pourtant, il découle de la décision n° 2005/532 DC du 19 janvier 2006 deux régimes distincts d'accès aux données relatives au trafic.

D'une part, le régime de l'ouverture du traitement dans le cadre de la répression des actes terroristes reste soumis

²⁴ CNIL, délibération n° 2005-208 du 10 octobre 2005, précitée.

²⁵ À cet égard la CNIL fait observer que « *l'obligation ainsi faite aux opérateurs de communiquer, dans le cadre des pouvoirs de police administrative et hors contrôle des autorités judiciaires, les traces des connexions qui, par recoupement avec d'autres données, peuvent dévoiler l'identité des utilisateurs d'internet, leur navigation sur le Web et, de manière plus générale, l'usage privé que l'on fait du réseau, déroge aux principes fondamentaux de protection des libertés individuelles* » pour conclure que « *dès lors, il convient que la loi édictant une telle obligation soit à la fois claire et précise et que le dispositif mis en œuvre soit adapté et proportionné* », CNIL, délibération n° 2005-208 du 10 octobre 2005, précitée.

²⁶ Décision n° 2005-532 DC - 19 janvier 2006, précitée.

²⁷ Pour des illustrations voir, « *La réquisition administrative des données de connexion conforme à la constitution* », Legalis, 20 janvier 2006.

http://www.legalis.net/breves-article.php3?id_article=1562, document consulté le 29 janvier 2006.

Pour une opinion contraire voir, ROGER, P., « *Le Conseil Constitutionnel défend la séparation des pouvoirs* », Le Monde, 21 janvier 2006, p.10.

¹⁹ CNIL, délibération n° 2005-208 du 10 octobre 2005, précitée.

²⁰ « *Faisant suite à un proposition du parlement européen, en décembre 2004, la Commission a annoncé l'allocation de 7 millions d'euros à un projet pilote dans le domaine de la préparation et de la réponse aux attaques terroristes et leur prévention* », droit pénal n° 11, novembre 2005, alerte 90.

²¹ NUNO ALVARO, N., [rapport 2004/0813\(CNS\)](#) au Parlement européen pour la commission des libertés, de la justice et des affaires intérieures, précité.

²² Nouvel article L. 34-1 CPCE.

²³ Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, J.O n° 143 du 22 juin 2004, p. 11168.

au contrôle d'une autorité judiciaire. D'autre part, l'accès aux données relatives au trafic dans le cadre de la prévention des infractions, délits et crime fait l'objet d'un nouveau régime plus souple, puisque exercé sans contrôle par une autorité judiciaire. En effet, l'autorité de contrôle sera alors une « *personnalité qualifiée* » placée auprès du ministre de l'intérieur par la CNCIS pour une durée de trois ans renouvelable. C'est cependant le ministre de l'intérieur qui choisit cette « *personnalité qualifiée* » dans une liste d'au moins trois noms. Celle-ci établit un rapport d'activité annuel adressé à la CNCIS. Le régime est incontestablement plus souple, le contrôle étant très lié à l'autorité de tutelle, c'est-à-dire au ministre de l'intérieur.

La dualité de régime s'expose, au moins dans un premier temps, à ne pas toujours être bien perçue par le débiteur de l'obligation de conservation. En effet, ces derniers ne sont pas nécessairement en mesure, surtout dans le cadre de petites structures, de savoir si la réquisition est administrative et s'inscrit dans le cadre de la prévention ou, s'il s'agit de la répression de comportements délictueux, qui nécessite le contrôle d'une autorité judiciaire. En outre, il est permis de s'interroger quant à la capacité d'un « Cybercafé » à s'opposer à une réquisition qu'il estime illicite. Quelles seront les voies de recours ? Celles-ci existent puisque le Conseil Constitutionnel considère « *que les personnes ayant un intérêt à agir ne sont pas privées par la disposition critiquée des garanties juridictionnelles de droit commun dont sont assorties les mesures de police administrative ; que leur droit au recours n'est donc pas méconnu* ». En pratique, un petit établissement s'opposera-t-il à une réquisition au risque de s'attirer la rancune des demandeurs ? Sera-t-il à même de discerner où s'arrête la prévention et où commence la répression ? Enfin, le nouveau régime français sera-t-il conforme à la directive communautaire qui devrait être prochainement adoptée²⁸ ? Le décret d'application de la loi nouvelle, dont l'adoption est prévue dans le courant du mois de février 2006, devrait apporter quelques éléments de réponse supplémentaires. Il semble toutefois acquis que les définitions larges données par la loi nouvelle posent d'ores et déjà des difficultés d'interprétations, qui devront être levées non seulement par la voie réglementaire, mais encore par les juridictions qui auront à connaître d'éventuels contentieux.



²⁸ Pour suivre l'évolution du projet de directive, voir LE CLAINCHE, J., « *Vers une durée de rétention sans... retenue ?* », précité. Voir également, 2005 et à LE CLAINCHE, J., « *Désaccord entre le Conseil et la Commission sur la durée de conservation des données de trafic* », précité et LE CLAINCHE, J. « *Toujours pas de consensus sur la rétention des données relatives au trafic* », précité.

Décision n° 2005-532 DC du 19 janvier 2006 Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

Thèmes

Informatique et libertés, Droit pénal

Abstract

Lutte contre le terrorisme, droits de la défense, réquisition administrative de données techniques de connexion, accès sous contrôle d'une autorité judiciaire (non), séparation des pouvoirs; liberté d'aller et venir, inconstitutionnalité (oui)

Résumé

Décision du Conseil Constitutionnel au sujet de la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

Décision

Décision n° 2005-532 DC du 19 janvier 2006

Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

Le Conseil constitutionnel a été saisi, dans les conditions prévues à l'article 61, deuxième alinéa, de la Constitution, de la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, le 23 décembre 2005, par M. Jean-Pierre BEL, Mmes Jacqueline ALQUIER, Michèle ANDRÉ, MM. Bernard ANGELS, Bertrand AUBAN, Mme Maryse BERGÉ-LAVIGNE, M. Jean BESSON, Mme Marie-Christine BLANDIN, MM. Yannick BODIN, Didier BOULAUD, Mmes Alima BOUMEDIENE-THIERY, Yolande BOYER, Nicole BRICQ, MM. Jean-Louis CARRÈRE, Bernard CAZEAU, Michel CHARASSE, Pierre-Yves COLLOMBAT, Roland COURTEAU, Yves DAUGE, Jean-Pierre DEMERLIAT, Mme Christiane DEMONTÈS, MM. Jean DESESSARD, Claude DOMEIZEL, Michel DREYFUS-SCHMIDT, Mme Josette DURRIEU, MM. Bernard DUSSAUT, Jean-Claude FRÉCON, Bernard FRIMAT, Charles GAUTIER, Mme Odette HERVIAUX, MM. Yves KRATTINGER, Serge LAGAUCHE, Louis LE PENSEC, André LEJEUNE, Roger MADEC, Jacques MAHÉAS, François MARC, Jean-Pierre MASSERET, Marc MASSION, Pierre MAUROY, Jean-Luc MÉLENCHON, Louis MERMAZ, Jean-Pierre MICHEL, Gérard MIQUEL, Michel MOREIGNE, Jean-Marc PASTOR, Jean-Claude PEYRONNET, Jean-François PICHERAL, Bernard PIRAS, Mme Gisèle PRINTZ, MM. Daniel RAOUL, Paul RAOULT, Daniel REINER, Thierry REPENTIN, Roland

RIES, Gérard ROUJAS, Mme Patricia SCHILLINGER, MM. Michel SERGENT, Jacques SIFFRE, René-Pierre SIGNÉ, Jean-Pierre SUEUR, Michel TESTON, Jean-Marc TODESCHINI, André VANTOMME et Richard YUNG, sénateurs ;

LE CONSEIL CONSTITUTIONNEL,

Vu la Constitution ;

Vu l'ordonnance n° 58-1067 du 7 novembre 1958 modifiée, portant loi organique sur le Conseil constitutionnel ;

Vu le code des douanes ;

Vu le code pénal ;

Vu le code des postes et des communications électroniques ;

Vu le code de procédure pénale ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 95-73 du 21 janvier 1995 modifiée, d'orientation et de programmation relative à la sécurité ;

Vu la loi n° 2003-239 du 18 mars 2003 modifiée, pour la sécurité intérieure ;

Vu la loi n° 2004-575 du 21 juin 2004 modifiée, pour la confiance dans l'économie numérique ;

Vu les observations du Gouvernement, enregistrées le 10 janvier 2006 ;

Le rapporteur ayant été entendu ;

1. Considérant que les sénateurs requérants défèrent au Conseil constitutionnel la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers ; qu'ils contestent la conformité à la Constitution de ses articles 6 et 8 ; qu'ils font également valoir que le Parlement aurait adopté des dispositions n'ayant pas leur place dans la loi déférée ;

- SUR L'ARTICLE 6 :

2. Considérant que le I de l'article 6 de la loi déferée insère dans le code des postes et des communications électroniques un nouvel article L. 34-1-1 qui institue, " **afin de prévenir et de réprimer les actes de terrorisme** ", une **procédure de réquisition administrative de données techniques de connexion** ; que cette procédure sera mise en oeuvre par des **"agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions"** ; qu'elle s'appliquera à toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau ; qu'elle sera limitée " aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date de la communication " ; qu'elle sera subordonnée à un accord préalable d'une personnalité désignée par la Commission nationale de contrôle des interceptions de sécurité ; qu'elle sera soumise au contrôle de cette commission, laquelle adressera des recommandations au ministre de l'intérieur lorsqu'elle constatera " un manquement aux règles édictées par le présent article ou une atteinte aux droits et libertés " ; qu'elle ouvrira droit à une compensation financière des surcoûts consécutifs aux demandes d'information ;

3. Considérant que le II de ce même article 6 complète l'article 6 de la loi du 21 juin 2004 susvisée par un II *bis* qui, " **afin de prévenir et de réprimer les actes de terrorisme** ", étend cette procédure de réquisition aux fournisseurs d'accès et d'hébergement ;

4. Considérant que les requérants font valoir que cette nouvelle procédure est destinée non seulement à la prévention des délits et des crimes terroristes mais aussi à leur répression ; qu'ils en déduisent que, **dès lors qu'elle n'est pas placée sous la surveillance de l'autorité judiciaire, elle méconnaît tant la liberté individuelle que le droit à la vie privée** ; qu'ils dénoncent en outre une atteinte au droit au recours ;

5. Considérant que **les données techniques** que l'article 6 de la loi déferée autorise les services de police et de gendarmerie à requérir **peuvent déjà être obtenues, en application des dispositions du code de procédure pénale, dans le cadre d'opérations de police judiciaire destinées à constater les infractions à la loi pénale**, à en rassembler les preuves ou à en rechercher

les auteurs ; que, pour leur part, les réquisitions de données permises par les nouvelles dispositions constituent des mesures de police purement administrative ; qu'elles ne sont pas placées sous la direction ou la surveillance de l'autorité judiciaire, mais relèvent de la seule responsabilité du pouvoir exécutif ; qu'elles ne peuvent donc avoir d'autre finalité que de préserver l'ordre public et de prévenir les infractions ; que, dès lors, **en indiquant qu'elles visent non seulement à prévenir les actes de terrorisme, mais encore à les réprimer, le législateur a méconnu le principe de la séparation des pouvoirs** ;

6. Considérant qu'il y a lieu, par suite, de déclarer **contraires à la Constitution les mots : " et de réprimer "** figurant au deuxième alinéa du I de l'article 6 de la loi déferée, ainsi qu'au deuxième alinéa de son II ; que demeure néanmoins l'obligation qui incombe à toute autorité administrative, lorsqu'elle acquiert la connaissance d'un crime ou d'un délit, d'en aviser l'autorité judiciaire ;

7. Considérant que les mots ainsi déclarés contraires à la Constitution sont séparables des autres dispositions de l'article 6 de la loi déferée ; qu'il y a lieu, en conséquence, de poursuivre l'examen de la conformité de ces dernières aux règles et principes de valeur constitutionnelle ;

8. Considérant, en premier lieu, que l'article 66 de la Constitution, aux termes duquel : " *Nul ne peut être arbitrairement détenu. - L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi* ", ne saurait être méconnu par une disposition qui se borne à instaurer une procédure de réquisition de données techniques ;

9. Considérant, en deuxième lieu, qu'il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent le respect de la vie privée et la liberté d'entreprendre, respectivement protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789 ;

10. Considérant, en l'espèce, que le législateur a assorti la procédure de réquisition de données techniques qu'il a instituée de limitations et précautions, précisées ci-dessus, propres à assurer la conciliation qui lui incombe entre, d'une part, le respect de la vie privée des personnes et la liberté d'entreprendre des opérateurs, et, d'autre part, la prévention des actes terroristes, à laquelle concourt ladite procédure ;

11. Considérant, enfin, qu'aux termes de l'article 16 de la Déclaration de 1789 : " *Toute société dans laquelle la*

garantie des droits n'est pas assurée ni la séparation des pouvoirs déterminée, n'a point de Constitution " ; qu'il résulte de cette disposition qu'il ne doit pas être porté d'atteintes substantielles au droit des personnes intéressées d'exercer un recours effectif devant une juridiction ;

12. Considérant, en l'espèce, que les personnes ayant un intérêt à agir ne sont pas privées par la disposition critiquée des garanties juridictionnelles de droit commun dont sont assorties les mesures de police administrative ; que leur droit au recours n'est donc pas méconnu ;

13. Considérant qu'il résulte de tout ce qui précède qu'à l'exception des mots : " *et de réprimer* " figurant aux deuxièmes alinéas du I et du II de l'article 6 de la loi déferée, celui-ci n'est pas contraire à la Constitution ;

- SUR L'ARTICLE 8 :

14. Considérant que l'article 8 de la loi déferée donne une nouvelle rédaction à l'article 26 de la loi du 18 mars 2003 susvisée ; qu'il **permet aux services de police, de gendarmerie ou des douanes de mettre en oeuvre " des dispositifs fixes ou mobiles de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants, en tous points appropriés du territoire..."** ; qu'il prévoit que " *l'emploi de tels dispositifs est également possible par les services de police et de gendarmerie nationales, à titre temporaire, pour la préservation de l'ordre public, à l'occasion d'événements particuliers ou de grands rassemblements de personnes, par décision de l'autorité administrative* " ; qu'il précise que les données ainsi collectées peuvent faire l'objet de traitements automatisés ; qu'il détermine les conditions de leur exploitation et de leur conservation, en fonction du résultat du rapprochement effectué avec les traitements automatisés de données relatifs aux véhicules volés ou signalés ;

15. Considérant que, selon les requérants, ces dispositions, en organisant " **un système généralisé de contrôle** " qui s'étend aux personnes occupant les véhicules concernés, méconnaissent l'article 66 de la Constitution, la liberté d'aller et venir, ainsi que le respect de la vie privée ; qu'ils soutiennent également qu'elles sont entachées d'**incompétence négative** ;

16. Considérant, en premier lieu, que, par sa nature même, la procédure de recueil automatisé de données relatives aux véhicules instituée par l'article 8 de la loi déferée ne saurait porter atteinte ni à la règle, posée par l'article 66 de la Constitution, selon laquelle nul ne peut être arbitrairement détenu, ni à la liberté d'aller et venir protégée par les articles 2 et 4 de la Déclaration de 1789 ;

17. Considérant, en deuxième lieu, que le dispositif en cause peut être utilisé tant pour des opérations de police administrative que pour des opérations de police judiciaire ; qu'il se trouve placé, à ce dernier titre, sous le contrôle de l'autorité judiciaire ; qu'ainsi, en assignant à ce dispositif la mission de faciliter la répression des infractions, l'article contesté, à la différence de l'article 6 précédemment examiné, **ne porte pas atteinte au principe de la séparation des pouvoirs** ;

18. Considérant, en troisième lieu, qu'il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public, notamment à la sécurité des personnes et des biens, et la recherche d'auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figure le respect de la vie privée ;

19. Considérant qu'en adoptant les dispositions contestées, le législateur a entendu, d'une part, prévenir et réprimer le terrorisme et les infractions qui lui sont liées, d'autre part, faciliter la constatation des crimes, des infractions liées à la criminalité organisée, du vol et recel de véhicules et de certains délits douaniers ; qu'il leur a également assigné comme finalité la recherche des auteurs de ces infractions ;

20. Considérant que les enregistrements seront effacés au bout de huit jours si les caractéristiques permettant l'identification des véhicules, ainsi collectées, **ne figurent ni dans le fichier national des véhicules volés ou signalés, ni dans la partie du système d'information Schengen relative aux véhicules** ; que les critères de cette recherche seront les caractéristiques des véhicules et non les images des passagers ; que les données n'ayant pas fait l'objet d'un " *rapprochement positif* " ne pourront être consultées pendant ce délai, sous réserve des besoins résultant d'une procédure pénale ; que seules les données ayant fait l'objet de ce rapprochement seront conservées ; que **la durée de cette conservation ne pourra alors excéder un mois, sauf pour les besoins d'une procédure pénale ou douanière** ; que seuls auront accès au dispositif, dans les limites ci-dessus décrites, des agents des services de la police et de la gendarmerie nationales individuellement désignés et dûment habilités ; que les traitements automatisés des données recueillies seront soumis aux dispositions de la loi du 6 janvier 1978 susvisée ;

21. Considérant qu'eu égard aux finalités que s'est assignées le législateur et à l'ensemble des garanties qu'il a prévues, les dispositions contestées sont propres à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée ;

22. Considérant que les griefs dirigés contre l'article 8, lequel n'est pas entaché d'incompétence négative, doivent être rejetés ;

- SUR LA PLACE DE CERTAINES DISPOSITIONS DANS LA LOI DÉFÉRÉE :

23. Considérant que, selon les requérants, la loi déferée comporte " *de nombreuses dispositions étrangères à la répression du terrorisme* " ; qu'ils estiment que ces dispositions, issues d'amendements adoptés au cours du débat parlementaire, n'ont pas leur place dans ladite loi et doivent être déclarées contraires à la Constitution ;

24. Considérant qu'aux termes de l'article 6 de la Déclaration de 1789 : " *La loi est l'expression de la volonté générale...* " ; qu'aux termes du premier alinéa de l'article 34 de la Constitution : " *La loi est votée par le Parlement* " ; qu'aux termes du premier alinéa de son article 39 : " *L'initiative des lois appartient concurremment au Premier ministre et aux membres du Parlement* " ; que le droit d'amendement que la Constitution confère aux parlementaires et au Gouvernement est mis en oeuvre dans les conditions et sous les réserves prévues par ses articles 40, 41, 44, 45, 47 et 47-1 ;

25. Considérant, d'une part, qu'il résulte de la combinaison des dispositions précitées que le droit d'amendement qui appartient aux membres du Parlement et au Gouvernement doit pouvoir s'exercer pleinement au cours de la première lecture des projets et des propositions de loi par chacune des deux assemblées ; qu'il ne saurait être limité, à ce stade de la procédure et dans le respect des exigences de clarté et de sincérité du débat parlementaire, que par les règles de recevabilité ainsi que par la nécessité, pour un amendement, de ne pas être dépourvu de tout lien avec l'objet du texte déposé sur le bureau de la première assemblée saisie ;

26. Considérant, d'autre part, qu'il ressort également de l'économie de l'article 45 de la Constitution et notamment de son premier alinéa aux termes duquel : " *Tout projet ou proposition de loi est examiné successivement dans les deux assemblées du Parlement en vue de l'adoption d'un texte identique* ", que, comme le rappellent d'ailleurs les règlements de l'Assemblée nationale et du Sénat, les adjonctions ou modifications qui peuvent être apportées après la première lecture par les membres du Parlement et par le Gouvernement doivent être en relation directe avec une disposition restant en discussion ; que, toutefois, ne sont pas soumis à cette dernière obligation les amendements destinés à assurer le respect de la Constitution, à opérer une coordination avec des textes en cours d'examen ou à corriger une erreur matérielle ;

27. Considérant, par suite, que doivent être regardées comme adoptées selon une procédure irrégulière les adjonctions ou modifications apportées à un projet ou à

une proposition de loi dans des conditions autres que celles précisées ci-dessus ;

28. Considérant, en l'espèce, que la loi déferée n'a fait l'objet que d'une lecture par chacune des deux assemblées avant la réunion de la commission mixte paritaire ; que, dès lors, les dispositions qui ont été introduites au cours du débat parlementaire doivent satisfaire aux conditions applicables aux amendements adoptés durant la première lecture, notamment à la nécessité de ne pas être dépourvues de tout lien avec l'objet initial du projet de loi ;

29. Considérant que l'article 19 de la loi déferée, issu d'un amendement adopté par l'Assemblée nationale, insère, après le quatrième alinéa de l'article 19 de la loi du 21 janvier 1995 susvisée, un alinéa ainsi rédigé : " *La représentation syndicale au sein des commissions administratives paritaires compétentes pour les corps de fonctionnaires actifs des services de la police nationale peut déroger au statut général de la fonction publique afin d'adapter et de simplifier la gestion de ces personnels. A ce titre, les gardiens de la paix et les brigadiers de police constituent un collège électoral unique au sein des commissions administratives paritaires nationales et interdépartementales représentant le corps d'encadrement et d'application de la police nationale* " ;

30. Considérant que, contrairement aux autres dispositions de la loi déferée, l'article 19 précité est dépourvu de tout lien avec un projet de loi qui, lors de son dépôt sur le bureau de l'Assemblée nationale, première assemblée saisie, comportait exclusivement des mesures relatives à la lutte contre le terrorisme, à la sécurité et aux contrôles aux frontières ; qu'il suit de là que cet article 19 a été adopté selon une procédure contraire à la Constitution ;

31. Considérant qu'il n'y a lieu, pour le Conseil constitutionnel, de soulever d'office aucune question de conformité à la Constitution,

DÉCIDE :

Article premier.- Sont déclarés contraires à la Constitution :

- les mots : " et de réprimer " figurant aux deuxièmes alinéas du I et du II de l'article 6 de la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers,

- l'article 19 de la même loi.

Article 2.- Le surplus de l'article 6 et l'article 8 de la même loi ne sont pas contraires à la Constitution.

Article 3.- La présente décision sera publiée au *Journal officiel* de la République française.

Délibéré par le Conseil constitutionnel dans sa séance du 19 janvier 2006, où siégeaient : M. Pierre MAZEAUD, Président, MM. Jean-Claude COLLIARD, Olivier DUTHEILLET de LAMOTHE et Valéry GISCARD d'ESTAING, Mme Jacqueline de GUILLENCHMIDT, MM. Pierre JOXE et Jean-Louis PEZANT, Mme Dominique SCHNAPPER, M. Pierre STEINMETZ et Mme Simone VEIL.

La décision sur le site du Conseil Constitutionnel

Référence : Conseil Constitutionnel, décision du 19 janvier 2006, N° 2005-532 DC- LOI RELATIVE À LA LUTTE CONTRE LE TERRORISME ET PORTANT DISPOSITIONS DIVERSES RELATIVES À LA SÉCURITÉ ET AUX CONTRÔLES FRONTALIERS, DROIT-TIC

http://www.droit-tic.com/juris/aff.php?id_juris=63



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

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

J.O n° 20 du 24 janvier 2006 page 1129
texte n° 1.

NOR: INTX0500242L

L'Assemblée nationale et le Sénat ont adopté,

Vu la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006,

Le Président de la République promulgue la loi dont la teneur suit :

Chapitre Ier

Dispositions relatives à la vidéosurveillance

Article 1

L'article 10 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité est ainsi modifié :

1° Le deuxième alinéa du II est remplacé par deux alinéas ainsi rédigés :

« La même faculté est ouverte aux autorités publiques aux fins de prévention d'actes de terrorisme ainsi que, pour la protection des abords immédiats de leurs bâtiments et installations, aux autres personnes morales, dans les lieux susceptibles d'être exposés à des actes de terrorisme.

« Il peut être également procédé à ces opérations dans des lieux et établissements ouverts au public aux fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol ou sont susceptibles d'être exposés à des actes de terrorisme. » ;

2° Le III est ainsi modifié :

a) Après le deuxième alinéa, sont insérés quatre alinéas ainsi rédigés :

« L'autorisation peut prescrire que les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales sont destinataires des images et enregistrements. Elle précise alors les modalités de transmission des images et d'accès aux enregistrements ainsi que la durée de conservation des images, dans la limite d'un mois à compter de cette transmission ou de cet accès, sans préjudice des nécessités de leur conservation pour les besoins d'une procédure pénale. La décision de permettre aux agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales d'être destinataires des images et enregistrements peut également être prise à tout moment, après avis de la commission départementale, par arrêté préfectoral. Ce dernier précise alors les modalités de transmission des images et d'accès aux enregistrements. Lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent, cette décision peut être prise sans avis préalable de la commission départementale. Le président de la commission est immédiatement informé de cette décision qui fait l'objet d'un examen lors de la plus prochaine réunion de la commission.

« Les systèmes de vidéosurveillance installés doivent être conformes à des normes techniques définies par arrêté ministériel, à compter de l'expiration d'un délai de deux ans après la publication de l'acte définissant ces normes.

« Les systèmes de vidéosurveillance sont autorisés pour une durée de cinq ans renouvelable.

« La commission départementale instituée au premier alinéa peut à tout moment exercer, sauf en matière de défense nationale, un contrôle sur les conditions de fonctionnement des dispositifs autorisés en application des mêmes dispositions. Elle émet, le cas échéant, des recommandations et propose la suspension des dispositifs lorsqu'elle constate qu'il en est fait un usage anormal ou non conforme à leur autorisation. » ;

b) Le dernier alinéa est ainsi rédigé :

« Les autorisations mentionnées au présent III et délivrées antérieurement à la date de publication 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 sont réputées délivrées pour une durée de cinq ans à compter de cette date. » ;

3° Après le III, il est inséré un III bis ainsi rédigé :

« III bis. - Lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent, le représentant de l'Etat dans le département et, à Paris, le préfet de police peuvent délivrer aux personnes mentionnées au II, sans avis préalable de la commission départementale, une autorisation provisoire d'installation d'un système de vidéosurveillance, exploité dans les conditions prévues par le présent article, pour une durée maximale de quatre mois. Le président de la commission est immédiatement informé de cette décision. Il peut alors la réunir sans délai afin qu'elle donne un avis sur la mise en oeuvre de la procédure d'autorisation provisoire.

« Le représentant de l'Etat dans le département et, à Paris, le préfet de police recueillent l'avis de la commission départementale sur la mise en oeuvre du système de vidéosurveillance conformément à la procédure prévue au III et se prononcent sur son maintien. La commission doit rendre son avis avant l'expiration du délai de validité de l'autorisation provisoire. » ;

4° Au début du VI, après les mots : « Le fait », sont insérés les mots : « d'installer un système de vidéosurveillance ou de le maintenir sans autorisation, » ;

5° Le VII est ainsi rédigé :

« VII. - Un décret en Conseil d'Etat fixe les modalités d'application du présent article et notamment les conditions dans lesquelles le public est informé de l'existence d'un dispositif de vidéosurveillance ainsi que de l'identité de l'autorité ou de la personne responsable. Ce décret fixe également les conditions dans lesquelles les agents visés au III sont habilités à accéder aux enregistrements et les conditions dans lesquelles la commission départementale exerce son contrôle. »

Article 2

Après l'article 10 de la loi n° 95-73 du 21 janvier 1995 précitée, il est inséré un article 10-1 ainsi rédigé :

« Art. 10-1. - I. - Aux fins de prévention d'actes de terrorisme, le représentant de l'Etat dans le département et, à Paris, le préfet de police peuvent prescrire la mise en oeuvre, dans un délai qu'ils fixent, de systèmes de vidéosurveillance, aux personnes suivantes :

« - les exploitants des établissements, installations ou ouvrages mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ;

« - les gestionnaires d'infrastructures, les autorités et personnes exploitant des transports collectifs, relevant de l'activité de transport intérieur régie par la loi n° 82-1153 du 30 décembre 1982 d'orientation des transports intérieurs ;

« - les exploitants d'aéroports qui, n'étant pas visés aux deux alinéas précédents, sont ouverts au trafic international.

« II. - Préalablement à leur décision et sauf en matière de défense nationale, le représentant de l'Etat dans le département et, à Paris, le préfet de police saisissent pour avis la commission départementale instituée à l'article 10 quand cette décision porte sur une installation de vidéosurveillance filmant la voie publique ou des lieux et établissements ouverts au public.

« Les systèmes de vidéosurveillance installés en application du présent article sont soumis aux dispositions des quatrième et cinquième alinéas du II, des deuxième, troisième, quatrième et sixième alinéas du III, du IV, du V, du VI et du VII de l'article 10.

« III. - Lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent, le représentant de l'Etat dans le département et, à Paris, le préfet de police peuvent prescrire, sans avis préalable de la commission départementale, la mise en oeuvre d'un système de vidéosurveillance exploité dans les conditions prévues par le II du présent article. Quand cette décision porte sur une installation de vidéosurveillance filmant la voie publique ou des lieux ou établissements ouverts au public, le président de la commission est immédiatement informé de cette décision. Il peut alors la réunir sans délai afin qu'elle donne un avis sur la mise en oeuvre de la procédure de décision provisoire.

« Avant l'expiration d'un délai maximal de quatre mois, le représentant de l'Etat dans le département et, à Paris, le préfet de police recueillent l'avis de la commission départementale sur la mise en oeuvre du système de vidéosurveillance conformément à la procédure prévue au III de l'article 10 et se prononcent sur son maintien.

« IV. - Si les personnes mentionnées au I refusent de mettre en oeuvre le système de vidéosurveillance prescrit, le représentant de l'Etat dans le département et, à Paris, le préfet de police les mettent en demeure de procéder à cette installation dans le délai qu'ils fixent en tenant compte des contraintes particulières liées à l'exploitation des établissements, installations et ouvrages et, le cas échéant, de l'urgence.

« V. - Est puni d'une amende de 150 000 EUR le fait, pour les personnes mentionnées au I, de ne pas avoir pris les mesures d'installation du système de vidéosurveillance prescrit à l'expiration du délai défini par la mise en demeure mentionnée au IV. »

Chapitre II

Contrôle des déplacements et communication des

données techniques relatives aux échanges téléphoniques et électroniques des personnes susceptibles de participer à une action terroriste

Article 3

I. - Après la première phrase du huitième alinéa de l'article 78-2 du code de procédure pénale, sont insérées trois phrases ainsi rédigées :

« Lorsque ce contrôle a lieu à bord d'un train effectuant une liaison internationale, il peut être opéré sur la portion du trajet entre la frontière et le premier arrêt qui se situe au-delà des vingt kilomètres de la frontière. Toutefois, sur celles des lignes ferroviaires effectuant une liaison internationale et présentant des caractéristiques particulières de desserte, le contrôle peut également être opéré entre cet arrêt et un arrêt situé dans la limite des cinquante kilomètres suivants. Ces lignes et ces arrêts sont désignés par arrêté ministériel. »

II. - Dans la deuxième phrase du huitième alinéa du même article, les mots : « mentionnée ci-dessus » sont remplacés par les mots : « mentionnée à la première phrase du présent alinéa ».

Article 4

I. - Après l'article 25 de la loi n° 95-73 du 21 janvier 1995 précitée, il est inséré un article 25-1 ainsi rédigé :

« Art. 25-1. - Les personnels de la police nationale revêtus de leurs uniformes ou des insignes extérieurs et apparents de leur qualité sont autorisés à faire usage de matériels appropriés pour immobiliser les moyens de transport dans les cas suivants :

« - lorsque le conducteur ne s'arrête pas à leurs sommations ;

« - lorsque le comportement du conducteur ou de ses passagers est de nature à mettre délibérément en danger la vie d'autrui ou d'eux-mêmes ;

« - en cas de crime ou délit flagrant, lorsque l'immobilisation du véhicule apparaît nécessaire en raison du comportement du conducteur ou des conditions de fuite.

« Ces matériels doivent être conformes à des normes techniques définies par arrêté ministériel. »

II. - 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 est abrogée.

Article 5

Le I de l'article L. 34-1 du code des postes et des communications électroniques est complété par un alinéa ainsi rédigé :

« 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, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article. »

Article 6

I. - Après l'article L. 34-1 du code des postes et des communications électroniques, il est inséré un article L. 34-1-1 ainsi rédigé :

« Art. L. 34-1-1. - Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au I de l'article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article.

« Les données pouvant faire l'objet de cette demande sont limitées aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

« Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnés au premier alinéa pour répondre à ces demandes font l'objet d'une compensation financière.

« Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée, placée auprès du ministre de l'intérieur. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité sur proposition du ministre de l'intérieur qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. 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.

« Cette instance peut à tout moment procéder à des contrôles relatifs aux opérations de communication des données techniques. Lorsqu'elle constate un manquement aux règles définies par le présent article ou une atteinte aux droits et libertés, elle saisit le ministre de l'intérieur d'une recommandation. Celui-ci lui fait connaître dans un délai de quinze jours les mesures qu'il a prises pour remédier aux manquements constatés.

« Les modalités d'application des dispositions du présent article sont fixées par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des données transmises. »

II. - Après le II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, il est inséré un II bis ainsi rédigé :

« II bis. - Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des prestataires mentionnés aux 1 et 2 du I la communication des données conservées et traitées par ces derniers en application du présent article.

« Les demandes des agents sont motivées et soumises à la décision de la personnalité qualifiée instituée par l'article L. 34-1-1 du code des postes et des communications électroniques selon les modalités prévues par le même article. La Commission nationale de contrôle des interceptions de sécurité exerce son contrôle selon les modalités prévues par ce même article.

« Les modalités d'application des dispositions du présent II bis sont fixées par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des données transmises. »

III. - 1. A la fin de la seconde phrase du premier alinéa de l'article 4 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, les mots : « ou de la personne que chacun d'eux aura spécialement déléguée » sont remplacés par les mots : « ou de l'une des deux personnes que chacun d'eux aura spécialement déléguées ».

2. Dans la première phrase du premier alinéa de l'article 19 de la même loi, les mots : « de l'article 14 et » sont remplacés par les mots : « de l'article 14 de la présente loi et au ministre de l'intérieur en application de l'article L. 34-1-1 du code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que ».

3. La même loi est complétée par un titre V intitulé : « Dispositions finales » comprenant l'article 27 qui devient l'article 28.

4. Il est inséré, dans la même loi, un titre IV ainsi rédigé :

« TITRE IV

« COMMUNICATION DES DONNÉES TECHNIQUES RELATIVES À DES COMMUNICATIONS ÉLECTRONIQUES

« Art. 27. - La Commission nationale de contrôle des interceptions de sécurité exerce les attributions définies à l'article L. 34-1-1 du code des postes et des communications électroniques et à l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique en ce qui concerne les demandes de communication de données formulées auprès des opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du code précité ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée. »

Chapitre III

Dispositions relatives aux traitements automatisés

de données à caractère personnel

Article 7

I. - Afin d'améliorer le contrôle aux frontières et de lutter contre l'immigration clandestine, le ministre de l'intérieur est autorisé à procéder à la mise en oeuvre de traitements automatisés de données à caractère personnel, recueillies à l'occasion de déplacements internationaux en provenance ou à destination d'Etats n'appartenant pas à l'Union européenne, à l'exclusion des données relevant du I de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés :

1° Figurant sur les cartes de débarquement et d'embarquement des passagers de transporteurs aériens ;

2° Collectées à partir de la bande de lecture optique des documents de voyage, de la carte nationale d'identité et des visas des passagers de transporteurs aériens, maritimes ou ferroviaires ;

3° Relatives aux passagers et enregistrées dans les systèmes de réservation et de contrôle des départs lorsqu'elles sont détenues par les transporteurs aériens, maritimes ou ferroviaires.

Les traitements mentionnés au premier alinéa sont soumis aux dispositions de la loi n° 78-17 du 6 janvier 1978 précitée.

II. - Les traitements mentionnés au I peuvent également être mis en oeuvre dans les mêmes conditions aux fins de prévenir et de réprimer des actes de terrorisme. L'accès à ceux-ci est alors limité aux agents individuellement désignés et dûment habilités :

- des services de police et de gendarmerie nationales spécialement chargés de ces missions ;

- des services de police et de gendarmerie nationales ainsi que des douanes, chargés de la sûreté des transports internationaux.

III. - Les traitements mentionnés aux I et II peuvent faire l'objet d'une interconnexion avec le fichier des personnes recherchées et le système d'information Schengen.

IV. - Pour la mise en oeuvre des traitements mentionnés aux I et II, les transporteurs aériens sont tenus de recueillir et de transmettre aux services du ministère de l'intérieur les données énumérées au 2 de l'article 3 de la directive 2004/82/CE du Conseil, du 29 avril 2004, concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, et mentionnées au 3° du I.

Ils sont également tenus de communiquer aux services mentionnés à l'alinéa précédent les données du 3° du I autres que celles mentionnées au même alinéa lorsqu'ils les détiennent.

Les obligations définies aux deux alinéas précédents sont applicables aux transporteurs maritimes et ferroviaires.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités de transmission des données mentionnées au 3° du I.

V. - Est puni d'une amende d'un montant maximum de 50 000 EUR pour chaque voyage le fait pour une entreprise de transport aérien, maritime ou ferroviaire de méconnaître les obligations fixées au IV.

Le manquement est constaté par un procès-verbal établi par un fonctionnaire appartenant à l'un des corps dont la liste est définie par décret en Conseil d'Etat. Copie du procès-verbal est remise à l'entreprise de transport intéressée. Le manquement ainsi relevé donne lieu à une amende prononcée par l'autorité administrative compétente. L'amende est prononcée pour chaque voyage ayant donné lieu au manquement. Son montant est versé au Trésor public par l'entreprise de transport.

L'entreprise de transport a accès au dossier. Elle est mise à même de présenter ses observations écrites dans un délai d'un mois sur le projet de sanction. La décision de l'autorité administrative est susceptible d'un recours de pleine juridiction.

L'autorité administrative ne peut infliger d'amende à raison de faits remontant à plus d'un an.

VI. - Les transporteurs aériens, maritimes et ferroviaires ont obligation d'informer les personnes concernées par le traitement mis en oeuvre au titre du 3° du I du présent article conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 précitée.

Article 8

L'article 26 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure est ainsi rédigé :

« Art. 26. - Afin de prévenir et de réprimer le terrorisme, de faciliter la constatation des infractions s'y rattachant, de faciliter la constatation des infractions criminelles ou liées à la criminalité organisée au sens de l'article 706-73 du code de procédure pénale, des infractions de vol et de recel de véhicules volés, des infractions de contrebande, d'importation ou d'exportation commises en bande organisée, prévues et réprimées par le deuxième alinéa de l'article 414 du code des douanes, ainsi que la constatation, lorsqu'elles portent sur des fonds provenant de ces mêmes infractions, de la réalisation ou de la tentative de réalisation des opérations financières définies à l'article 415 du même code et afin de permettre le rassemblement des preuves de ces infractions et la recherche de leurs auteurs, les services de police et de gendarmerie nationales et des douanes peuvent mettre en oeuvre des dispositifs fixes ou mobiles de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants, en tous points appropriés du territoire, en particulier dans les zones frontalières, portuaires ou aéroportuaires ainsi que sur les grands axes de transit national ou international.

« L'emploi de tels dispositifs est également possible par les services de police et de gendarmerie nationales, à titre temporaire, pour la préservation de l'ordre public, à l'occasion d'événements particuliers ou de grands rassemblements de personnes, par décision de l'autorité administrative.

« Pour les finalités mentionnées au présent article, les données à caractère personnel collectées à l'occasion des contrôles susmentionnés peuvent faire l'objet de traitements automatisés mis en oeuvre par les services de police et de gendarmerie nationales et soumis aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

« Ces traitements comportent une consultation du traitement automatisé des données relatives aux véhicules volés ou signalés ainsi que du système d'information Schengen.

« Afin de permettre cette consultation, les données collectées sont conservées durant un délai maximum de huit jours au-delà duquel elles sont effacées dès lors qu'elles n'ont donné lieu à aucun rapprochement positif avec les traitements mentionnés au précédent alinéa. Durant cette période de huit jours, la consultation des données n'ayant pas fait l'objet d'un rapprochement positif avec ces traitements est interdite, sans préjudice des nécessités de leur consultation pour les besoins d'une procédure pénale. Les données qui font l'objet d'un rapprochement positif avec ces mêmes traitements sont conservées pour une durée d'un mois sans préjudice des nécessités de leur conservation pour les besoins d'une procédure pénale ou douanière.

« Aux fins de prévenir et de réprimer les actes de terrorisme et de faciliter la constatation des infractions s'y rattachant, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent avoir accès à ces traitements. »

Article 9

Pour les besoins de la prévention et de la répression des actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent, dans les conditions fixées par la loi n° 78-17 du 6 janvier 1978 précitée, avoir accès aux traitements automatisés suivants :

- le fichier national des immatriculations ;
- le système national de gestion des permis de conduire ;
- le système de gestion des cartes nationales d'identité ;
- le système de gestion des passeports ;
- le système informatisé de gestion des dossiers des ressortissants étrangers en France ;
- les données à caractère personnel, mentionnées aux articles L. 611-3 à L. 611-5 du code de l'entrée et du

séjour des étrangers et du droit d'asile, relatives aux ressortissants étrangers qui, ayant été contrôlés à l'occasion du franchissement de la frontière, ne remplissent pas les conditions d'entrée requises ;

- les données à caractère personnel mentionnées à l'article L. 611-6 du même code.

Pour les besoins de la prévention des actes de terrorisme, les agents des services de renseignement du ministère de la défense individuellement désignés et dûment habilités sont également autorisés, dans les conditions fixées par la loi n° 78-17 du 6 janvier 1978 précitée, à accéder aux traitements automatisés mentionnés ci-dessus.

Un arrêté du ministre de l'intérieur et du ministre de la défense détermine les services de renseignement du ministère de la défense qui sont autorisés à consulter lesdits traitements automatisés.

Article 10

Dans le 3° du I de l'article 23 de la loi n° 2003-239 du 18 mars 2003 précitée, les références : « 3° et 11° » sont remplacées par les références : « 3°, 6°, 11°, 12°, 13° et 14° ».

Chapitre IV

Dispositions relatives à la répression du terrorisme

et à l'exécution des peines

Article 11

I. - Après l'article 421-5 du code pénal, il est inséré un article 421-6 ainsi rédigé :

« Art. 421-6. - Les peines sont portées à vingt ans de réclusion criminelle et 350 000 EUR d'amende lorsque le groupement ou l'entente définie à l'article 421-2-1 a pour objet la préparation :

« 1° Soit d'un ou plusieurs crimes d'atteintes aux personnes visés au 1° de l'article 421-1 ;

« 2° Soit d'une ou plusieurs destructions par substances explosives ou incendiaires visées au 2° de l'article 421-1 et devant être réalisées dans des circonstances de temps ou de lieu susceptibles d'entraîner la mort d'une ou plusieurs personnes ;

« 3° Soit de l'acte de terrorisme défini à l'article 421-2 lorsqu'il est susceptible d'entraîner la mort d'une ou plusieurs personnes.

« Le fait de diriger ou d'organiser un tel groupement ou une telle entente est puni de trente ans de réclusion

criminelle et 500 000 EUR d'amende.

« Les deux premiers alinéas de l'article 132-23 relatifs à la période de sûreté sont applicables aux crimes prévus par le présent article. »

II. - Dans le premier alinéa des articles 78-2-2 et 706-16 et le 11° de l'article 706-73 du code de procédure pénale, la référence : « 421-5 » est remplacée par la référence : « 421-6 ».

Article 12

L'article 706-24 du code de procédure pénale est ainsi rétabli :

« Art. 706-24. - Les officiers et agents de police judiciaire, affectés dans les services de police judiciaire spécialement chargés de la lutte contre le terrorisme, peuvent être nominativement autorisés par le procureur général près la cour d'appel de Paris à procéder aux investigations relatives aux infractions entrant dans le champ d'application de l'article 706-16, en s'identifiant par leur numéro d'immatriculation administrative. Ils peuvent être autorisés à déposer ou à comparaître comme témoins sous ce même numéro.

« L'état civil des officiers et agents de police judiciaire visés au premier alinéa ne peut être communiqué que sur décision du procureur général près la cour d'appel de Paris. Il est également communiqué, à sa demande, au président de la juridiction de jugement saisie des faits.

« Les dispositions de l'article 706-84 sont applicables en cas de révélation de l'identité de ces officiers ou agents de police judiciaire, hors les cas prévus à l'alinéa précédent.

« Aucune condamnation ne peut être prononcée sur le seul fondement d'actes de procédure effectués par des enquêteurs ayant bénéficié des dispositions du présent article et dont l'état civil n'aurait pas été communiqué, à sa demande, au président de la juridiction saisie des faits.

« Les modalités d'application du présent article sont, en tant que de besoin, précisées par décret en Conseil d'Etat. »

Article 13

Le I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 précitée est complété par un alinéa ainsi rédigé :

« Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. Un décret en Conseil

d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum. »

Article 14

I. - Après l'article 706-22 du code de procédure pénale, il est inséré un article 706-22-1 ainsi rédigé :

« Art. 706-22-1. - Par dérogation aux dispositions de l'article 712-10, sont seuls compétents le juge de l'application des peines du tribunal de grande instance de Paris, le tribunal de l'application des peines de Paris et la chambre de l'application des peines de la cour d'appel de Paris pour prendre les décisions concernant les personnes condamnées pour une infraction entrant dans le champ d'application de l'article 706-16, quel que soit le lieu de détention ou de résidence du condamné.

« Ces décisions sont prises après avis du juge de l'application des peines compétent en application de l'article 712-10.

« Pour l'exercice de leurs attributions, les magistrats des juridictions mentionnées au premier alinéa peuvent se déplacer sur l'ensemble du territoire national, sans préjudice de l'application des dispositions de l'article 706-71 sur l'utilisation de moyens de télécommunication. »

II. - Les dispositions du présent article entreront en vigueur le 1er mai 2006.

Article 15

Le premier alinéa de l'article 706-25 du code de procédure pénale est complété par une phrase ainsi rédigée :

« Pour le jugement des accusés mineurs âgés de seize ans au moins, les règles relatives à la composition et au fonctionnement de la cour d'assises des mineurs sont également fixées par ces dispositions, deux des assesseurs étant pris parmi les juges des enfants du ressort de la cour d'appel, conformément aux dispositions de l'article 20 de l'ordonnance n° 45-174 du 2 février 1945 relative à l'enfance délinquante, dont les huitième à quatorzième alinéas sont applicables. »

Article 16

I. - L'article 16 du code de procédure pénale est ainsi modifié :

1° Dans le 3°, les mots : « ; les fonctionnaires titulaires du corps de commandement et d'encadrement de la police nationale et les fonctionnaires stagiaires du corps de commandement et d'encadrement déjà titulaires de cette qualité, nominativement désignés par arrêté des ministres de la justice et de l'intérieur après avis conforme d'une commission » sont remplacés par les mots : « et les officiers de police » ;

2° Dans le 4°, les mots : « de maîtrise » sont remplacés par les mots : « d'encadrement », et les mots : « de la commission mentionnée au 3° » sont remplacés par les mots : « d'une commission » ;

3° Dans le sixième alinéa, les références : « 2° à 4° » sont remplacées par les références : « 2° et 4° ».

II. - Les 2° et 3° de l'article 20 du même code sont remplacés par un 2° ainsi rédigé :

« 2° Les fonctionnaires titulaires du corps d'encadrement et d'application de la police nationale n'ayant pas la qualité d'officier de police judiciaire, sous réserve des dispositions concernant les fonctionnaires visés aux 4° et 5° ci-après ; ».

Article 17

L'article 706-88 du code de procédure pénale est complété par quatre alinéas ainsi rédigés :

« S'il ressort des premiers éléments de l'enquête ou de la garde à vue elle-même qu'il existe un risque sérieux de l'imminence d'une action terroriste en France ou à l'étranger ou que les nécessités de la coopération internationale le requièrent impérativement, le juge des libertés peut, à titre exceptionnel et selon les modalités prévues au deuxième alinéa, décider que la garde à vue en cours d'une personne, se fondant sur l'une des infractions visées au 11° de l'article 706-73, fera l'objet d'une prolongation supplémentaire de vingt-quatre heures, renouvelable une fois.

« A l'expiration de la quatre-vingt-seizième heure et de la cent-vingtième heure, la personne dont la prolongation de la garde à vue est ainsi décidée peut demander à s'entretenir avec un avocat, selon les modalités prévues par l'article 63-4. La personne gardée à vue est avisée de ce droit dès la notification de la prolongation prévue au présent article.

« Outre la possibilité d'examen médical effectué à l'initiative du gardé à vue, dès le début de chacune des deux prolongations supplémentaires, il est obligatoirement examiné par un médecin désigné par le procureur de la République, le juge d'instruction ou l'officier de police judiciaire. Le médecin requis devra se prononcer sur la compatibilité de la prolongation de la mesure avec l'état de santé de l'intéressé.

« S'il n'a pas été fait droit à la demande de la personne gardée à vue de faire prévenir, par téléphone, une personne avec laquelle elle vit habituellement ou l'un de ses parents en ligne directe, l'un de ses frères et soeurs ou son employeur, de la mesure dont elle est l'objet, dans les conditions prévues aux articles 63-1 et 63-2, elle peut réitérer cette demande à compter de la quatre-vingt-seizième heure. »

Article 18

Dans l'article 800 du code de procédure pénale, après les mots : « en établit le tarif », sont insérés les mots : « ou fixe les modalités selon lesquelles ce tarif est établi ».

Article 19

[Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006.]

Chapitre V

Dispositions relatives aux victimes

d'actes de terrorisme

Article 20

Le premier alinéa de l'article L. 126-1 du code des assurances est ainsi modifié :

1° Les mots : « national et les » sont remplacés par les mots : « national, les » ;

2° Après les mots : « mêmes actes », les mots : « , sont indemnisées » sont remplacés par les mots : « ainsi que leurs ayants droit, quelle que soit leur nationalité, sont indemnisés ».

Chapitre VI

Dispositions relatives à la déchéance

de la nationalité française

Article 21

L'article 25-1 du code civil est complété par un alinéa ainsi rédigé :

« Si les faits reprochés à l'intéressé sont visés au 1° de l'article 25, les délais mentionnés aux deux alinéas précédents sont portés à quinze ans. »

Chapitre VII

Dispositions relatives à l'audiovisuel

Article 22

La loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication est ainsi modifiée :

1° L'article 33-1 est complété par un III ainsi rédigé :

« III. - Par dérogation aux I et II du présent article, les services de télévision relevant de la compétence de la France en application des articles 43-4 et 43-5 peuvent être diffusés par les réseaux n'utilisant pas des fréquences assignées par le Conseil supérieur de l'audiovisuel sans formalité préalable. Ils demeurent soumis aux obligations résultant de la présente loi et au contrôle du Conseil supérieur de l'audiovisuel, qui peut notamment utiliser à leur égard les procédures prévues aux articles 42, 42-1 et 42-10. Les opérateurs satellitaires dont l'activité a pour effet de faire relever des services de télévision de la compétence de la France, en application de l'article 43-4, et les distributeurs de services visés à l'article 34 sont tenus d'informer les éditeurs des services considérés du régime qui leur est applicable.

« Les conventions conclues entre le Conseil supérieur de l'audiovisuel et les éditeurs de services de télévision relevant de la compétence de la France en application des articles 43-4 et 43-5 sont réputées caduques à compter de l'entrée en vigueur 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. » ;

2° Au début du 1° de l'article 42-1, les mots : « La suspension de l'édition ou de la distribution » sont remplacés par les mots : « La suspension de l'édition, de la diffusion ou de la distribution » ;

3° La deuxième phrase de l'article 42-6 est complétée par les mots : « et, en cas de suspension de la diffusion d'un service, aux opérateurs satellitaires qui assurent la diffusion du service en France et qui devront assurer l'exécution de la mesure » ;

4° Le premier alinéa de l'article 43-6 est ainsi rédigé :

« Les services relevant de la compétence d'un autre Etat membre de la Communauté européenne ou partie à l'accord sur l'Espace économique européen peuvent être diffusés par les réseaux n'utilisant pas des fréquences assignées par le Conseil supérieur de l'audiovisuel sans formalité préalable. »

Chapitre VIII

Dispositions relatives à la lutte

contre le financement des activités terroristes

Article 23

I. - Le titre VI du livre V du code monétaire et financier est ainsi modifié :

1° Son intitulé est ainsi rédigé : « Obligations relatives à la lutte contre le blanchiment des capitaux et le financement des activités terroristes » ;

2° Dans l'article L. 562-10, après les mots : « et des délits », sont insérés les mots : « et de la lutte contre le financement des activités terroristes » ;

3° Le chapitre IV et les articles L. 564-1, L. 564-2 et L. 564-3 deviennent, respectivement, le chapitre V et les articles L. 565-1, L. 565-2 et L. 565-3 ;

4° Il est rétabli un chapitre IV ainsi rédigé :

« Chapitre IV

« Obligations relatives à la lutte

contre le financement des activités terroristes

« Art. L. 564-1. - Les organismes financiers et personnes mentionnés aux 1 à 5 et au 7 de l'article L. 562-1, qui détiennent ou reçoivent des fonds, instruments financiers et ressources économiques, sont tenus d'appliquer les mesures de gel ou d'interdiction prises en vertu du présent chapitre.

« Pour l'application du présent chapitre, on entend par fonds, instruments financiers et ressources économiques les avoirs de toute nature, corporels ou incorporels, mobiliers ou immobiliers, acquis par quelque moyen que ce soit, et les documents ou instruments légaux sous quelque forme que ce soit, y compris sous forme électronique ou numérique, qui prouvent un droit de propriété ou un intérêt sur ces avoirs, incluant, notamment, les crédits bancaires, les chèques de voyage, les chèques bancaires, les mandats, les actions, les titres, les obligations, les traites et les lettres de crédit.

« Art. L. 564-2. - Sans préjudice des mesures restrictives spécifiques prises en application de règlements du Conseil de l'Union européenne et des mesures prononcées par l'autorité judiciaire, le ministre chargé de l'économie peut décider le gel, pour une durée de six mois, renouvelable, de tout ou partie des fonds,

instruments financiers et ressources économiques détenus auprès des organismes et personnes mentionnés à l'article L. 564-1 qui appartiennent à des personnes physiques ou morales qui commettent, ou tentent de commettre, des actes de terrorisme, définis comme il est dit au 4 de l'article 1er du règlement (CE) n° 2580/2001 du Conseil, du 27 décembre 2001, concernant l'adoption de mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le terrorisme, les facilitent ou y participent et à des personnes morales détenues par ces personnes physiques ou contrôlées, directement ou indirectement, par elles au sens des 5 et 6 de l'article 1er du règlement (CE) n° 2580/2001 du Conseil, du 27 décembre 2001, précité. Les fruits produits par les fonds, instruments et ressources précités sont également gelés.

« Le gel des fonds, instruments financiers et ressources économiques détenus auprès des organismes et personnes mentionnés à l'article L. 564-1 s'entend comme toute action visant à empêcher tout mouvement, transfert ou utilisation de fonds, instruments financiers et ressources économiques qui auraient pour conséquence un changement de leur montant, de leur localisation, de leur propriété, de leur nature ou toute autre modification qui pourrait en permettre l'utilisation par les personnes faisant l'objet de la mesure de gel.

« Le ministre chargé de l'économie peut également décider d'interdire, pour une durée de six mois renouvelable, tout mouvement ou transfert de fonds, instruments financiers et ressources économiques au bénéfice des personnes physiques ou morales mentionnées au premier alinéa.

« Les décisions du ministre arrêtées en application du présent article sont publiées au Journal officiel et exécutoires à compter de la date de cette publication.

« Art. L. 564-3. - Les mesures de gel ou d'interdiction prises en vertu du présent chapitre s'imposent à toute personne copropriétaire des fonds, instruments et ressources précités, ainsi qu'à toute personne titulaire d'un compte joint dont l'autre titulaire est une personne propriétaire, nue-propriétaire ou usufruitière mentionnée au premier alinéa de l'article L. 564-2.

« Ces mesures sont opposables à tout créancier et à tout tiers pouvant invoquer des droits sur les fonds, instruments financiers et ressources économiques considérés même si l'origine de ces créances ou autres droits est antérieure à la publication de l'arrêté.

« Les mesures mentionnées au troisième alinéa de l'article L. 564-2 s'appliquent aux mouvements ou transferts de fonds, instruments financiers et ressources économiques dont l'ordre d'exécution a été émis antérieurement à la date de publication de la décision d'interdiction.

« Art. L. 564-4. - Le secret bancaire ou professionnel ne fait pas obstacle à l'échange d'informations entre les organismes et personnes mentionnés à l'article L. 564-1 et les services de l'Etat chargés de mettre en oeuvre une mesure de gel ou d'interdiction de mouvement ou de transfert des fonds, des instruments financiers et des ressources économiques lorsque ces informations visent à vérifier l'identité des personnes concernées directement ou indirectement par cette mesure. Les informations fournies ou échangées ne peuvent être utilisées qu'à ces fins.

« Les services de l'Etat chargés de mettre en oeuvre une mesure de gel ou d'interdiction de mouvement ou de transfert des fonds, des instruments financiers et ressources économiques et les autorités d'agrément et de contrôle des organismes et personnes mentionnés à l'article L. 564-1 sont autorisés à échanger les informations nécessaires à l'exercice de leurs missions respectives.

« Art. L. 564-5. - L'Etat est responsable des conséquences dommageables de la mise en oeuvre de bonne foi, par les organismes financiers et les personnes mentionnés à l'article L. 564-1, leurs dirigeants ou leurs préposés, des mesures de gel ou d'interdiction mentionnées à l'article L. 564-2. Aucune sanction professionnelle ne peut être prononcée à l'encontre de ces organismes et ces personnes, leurs dirigeants ou leurs préposés.

« Art. L. 564-6. - Un décret en Conseil d'Etat fixe les conditions d'application des dispositions du présent chapitre, notamment les conditions dans lesquelles les organismes et les personnes mentionnés à l'article L. 564-1 sont tenus d'appliquer les mesures de gel ou d'interdiction de mouvement ou de transfert des fonds, instruments financiers et ressources économiques prises en vertu du présent chapitre. »

II. - Le chapitre IV du titre VII du livre V du même code est ainsi modifié :

1° Son intitulé est ainsi rédigé : « Dispositions relatives à la lutte contre le blanchiment de capitaux et le financement des activités terroristes » ;

2° Il est ajouté un article L. 574-3 ainsi rédigé :

« Art. L. 574-3. - Est puni des peines prévues au 1 de l'article 459 du code des douanes le fait, pour les dirigeants ou les préposés des organismes financiers et personnes mentionnés à l'article L. 564-1 et, pour les personnes faisant l'objet d'une mesure de gel ou d'interdiction prise en application du chapitre IV du titre VI du présent livre, de se soustraire aux obligations en résultant ou de faire obstacle à sa mise en oeuvre.

« Sont également applicables les dispositions relatives à la constatation des infractions, aux poursuites, au

contentieux et à la répression des infractions des titres II et XII du code des douanes sous réserve des articles 453 à 459 du même code. »

III. - 1. A la fin de la dernière phrase du premier alinéa de l'article L. 563-1 du même code, la référence : « L. 564-1 » est remplacée par la référence : « L. 565-1 ».

2. Dans le dernier alinéa de l'article L. 563-4 du même code, la référence : « L. 564-2 » est remplacée par la référence : « L. 565-2 ».

Article 24

I. - L'article 321-6 du code pénal est ainsi rédigé :

« Art. 321-6. - Le fait de ne pas pouvoir justifier de ressources correspondant à son train de vie ou de ne pas pouvoir justifier de l'origine d'un bien détenu, tout en étant en relations habituelles avec une ou plusieurs personnes qui soit se livrent à la commission de crimes ou de délits punis d'au moins cinq ans d'emprisonnement et procurant à celles-ci un profit direct ou indirect, soit sont les victimes d'une de ces infractions, est puni d'une peine de trois ans d'emprisonnement et de 75 000 EUR d'amende.

« Est puni des mêmes peines le fait de faciliter la justification de ressources fictives pour des personnes se livrant à la commission de crimes ou de délits punis d'au moins cinq ans d'emprisonnement et procurant à celles-ci un profit direct ou indirect. »

II. - Après l'article 321-6 du même code, il est inséré un article 321-6-1 ainsi rédigé :

« Art. 321-6-1. - Les peines prévues par l'article 321-6 sont portées à cinq ans d'emprisonnement et 150 000 EUR d'amende lorsque les crimes et délits sont commis par un mineur sur lequel la personne ne pouvant justifier ses ressources a autorité.

« Elles sont portées à sept ans d'emprisonnement et 200 000 EUR d'amende lorsque les infractions commises constituent les crimes ou délits de traite des êtres humains, d'extorsion ou d'association de malfaiteurs, ou qu'elles constituent les crimes ou délits de trafic de stupéfiants, y compris en cas de relations habituelles avec une ou plusieurs personnes faisant usage de stupéfiants.

« Elles sont portées à dix ans d'emprisonnement et 300 000 EUR d'amende lorsqu'il s'agit d'une infraction mentionnée à l'alinéa précédent commise par un ou plusieurs mineurs. »

III. - Après l'article 321-10 du même code, il est inséré un article 321-10-1 ainsi rédigé :

« Art. 321-10-1. - Les personnes physiques coupables des délits prévus aux articles 321-6 et 321-6-1 encourent également la peine complémentaire de confiscation de tout ou partie de leurs biens, quelle qu'en soit la nature, meuble ou immeuble, divis ou indivis, dont elles n'ont pu justifier l'origine.

« Peuvent également être prononcées les peines complémentaires encourues pour les crimes ou les délits commis par la ou les personnes avec lesquelles l'auteur des faits était en relations habituelles. »

IV. - Les articles 222-39-1, 225-4-8, 312-7-1 et 450-2-1 du même code sont abrogés.

V. - L'article 706-73 du code de procédure pénale est complété par un 16° ainsi rédigé :

« 16° Délit de non-justification de ressources correspondant au train de vie, prévu par l'article 321-6-1 du code pénal, lorsqu'il est en relation avec l'une des infractions mentionnées aux 1° à 15°. »

VI. - 1. Dans l'article 313-5 du code de l'entrée et du séjour des étrangers et du droit d'asile, la référence : « 222-39-1 » est remplacée par la référence : « 321-6-1 ».

2. Dans l'article 450-5 du code pénal, la référence : « 450-2-1 » est remplacée par la référence : « 321-6-1 ».

3. Dans l'article 704 du code de procédure pénale, la référence : « 450-2-1 » est remplacée par la référence : « 321-6-1 ».

4. Dans le II de l'article 71 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, la référence : « 450-2-1 » est remplacée par la référence : « 321-6-1 ».

Chapitre IX

Dispositions relatives aux activités privées

de sécurité et à la sûreté aéroportuaire

Article 25

La loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de surveillance, de gardiennage et de transport de fonds est ainsi modifiée :

1° L'article 5 est ainsi modifié :

a) Le 5° est abrogé ;

b) Après le 8°, il est inséré un alinéa ainsi rédigé :

« L'agrément ne peut être délivré s'il résulte de l'enquête

administrative, ayant le cas échéant donné lieu à consultation des traitements de données à caractère personnel gérés par les services de police et de gendarmerie nationales relevant des dispositions de 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, que son comportement ou ses agissements sont contraires à l'honneur, à la probité, aux bonnes moeurs ou sont de nature à porter atteinte à la sécurité des personnes ou des biens, à la sécurité publique ou à la sûreté de l'Etat et sont incompatibles avec l'exercice des fonctions susmentionnées. »

2° Le 4° de l'article 6 est ainsi rédigé :

« 4° S'il résulte de l'enquête administrative, ayant le cas échéant donné lieu à consultation des traitements de données à caractère personnel gérés par les services de police et de gendarmerie nationales relevant des dispositions de l'article 26 de la loi n° 78-17 du 6 janvier 1978 précitée, à l'exception des fichiers d'identification, que son comportement ou ses agissements sont contraires à l'honneur, à la probité, aux bonnes moeurs ou sont de nature à porter atteinte à la sécurité des personnes ou des biens, à la sécurité publique ou à la sûreté de l'Etat et sont incompatibles avec l'exercice des fonctions susmentionnées ; »

3° L'article 22 est ainsi modifié :

a) Le 5° est abrogé ;

b) Après le 7°, il est inséré un alinéa ainsi rédigé :

« L'agrément ne peut être délivré s'il résulte de l'enquête administrative, ayant le cas échéant donné lieu à consultation des traitements de données à caractère personnel gérés par les services de police et de gendarmerie nationales relevant des dispositions de 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, que son comportement ou ses agissements sont contraires à l'honneur, à la probité, aux bonnes moeurs ou sont de nature à porter atteinte à la sécurité des personnes ou des biens, à la sécurité publique ou à la sûreté de l'Etat et sont incompatibles avec l'exercice des fonctions susmentionnées. » ;

4° Le 4° de l'article 23 est ainsi rédigé :

« 4° S'il résulte de l'enquête administrative, ayant le cas échéant donné lieu à consultation des traitements de données à caractère personnel gérés par les services de police et de gendarmerie nationales relevant des dispositions de l'article 26 de la loi n° 78-17 du 6 janvier 1978 précitée, à l'exception des fichiers d'identification, que son comportement ou ses agissements sont contraires à l'honneur, à la probité, aux bonnes moeurs ou sont de nature à porter atteinte à la sécurité des personnes ou des biens, à la sécurité publique ou à la

sûreté de l'Etat et sont incompatibles avec l'exercice des fonctions susmentionnées ; ».

Article 26

I. - Après l'article L. 213-4 du code de l'aviation civile, il est inséré un article L. 213-5 ainsi rédigé :

« Art. L. 213-5. - L'accès aux lieux de préparation et de stockage des biens et produits visés au premier alinéa de l'article L. 213-4 est soumis à la possession d'une habilitation délivrée par le représentant de l'Etat dans le département et, à Paris, par le préfet de police.

« L'enquête administrative diligentée aux fins d'instruction de la demande d'habilitation peut donner lieu à consultation du bulletin n° 2 du casier judiciaire et des traitements automatisés de données à caractère personnel gérés par les services de police et de gendarmerie nationales relevant des dispositions de 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. »

II. - Après l'article L. 321-7 du même code, il est inséré un article L. 321-8 ainsi rédigé :

« Art. L. 321-8. - L'accès aux lieux de traitement, de conditionnement et de stockage du fret et des colis postaux visés aux sixième et septième alinéas de l'article L. 321-7 est soumis à la possession d'une habilitation délivrée par le représentant de l'Etat dans le département et, à Paris, par le préfet de police.

« L'enquête administrative diligentée aux fins d'instruction de la demande d'habilitation peut donner lieu à consultation du bulletin n° 2 du casier judiciaire et des traitements automatisés de données à caractère personnel gérés par les services de police et de gendarmerie nationales relevant des dispositions de 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. »

Chapitre X

Dispositions relatives à l'outre-mer

Article 27

L'article 31 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité est ainsi rédigé :

« Art. 31. - Les dispositions de la présente loi sont applicables à Mayotte, à Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, en

Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, à l'exception des articles 6, 9, 11 à 14, 17, 18 et 24 ainsi que de l'article 23 pour ce qui concerne la Nouvelle-Calédonie et de l'article 33 pour ce qui concerne Mayotte, Saint-Pierre-et-Miquelon, les îles Wallis et Futuna, la Polynésie française et les Terres australes et antarctiques françaises, sous réserve des modifications suivantes :

« 1° Les dispositions de l'article 7 abrogées en vertu de l'article 12 de la loi n° 96-142 du 21 février 1996 relative à la partie législative du code général des collectivités territoriales restent en vigueur pour ce qui concerne Mayotte, Saint-Pierre-et-Miquelon, les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises ;

« 2° Dans les III et III bis de l'article 10 et les I, II, III et IV de l'article 10-1, les mots : "représentant de l'Etat dans le département sont remplacés par les mots : "représentant de l'Etat ;

« 3° Dans les III, III bis, V, VI et VII de l'article 10 et les II et III de l'article 10-1, les mots : "commission départementale sont remplacés par les mots : "commission locale ;

« 4° Pour leur application en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna :

« a) Dans le VI de l'article 10 et le V de l'article 10-1, le montant de l'amende en euros est remplacé par sa contre-valeur en monnaie locale ;

« b) A la fin du VI de l'article 10, les mots : "des articles 226-1 du code pénal et L. 120-2, L. 121-8 et L. 432-2-1 du code du travail sont remplacés par les mots : "de l'article 226-1 du code pénal ;

« c) Dans le troisième alinéa du I de l'article 10-1, les mots : "régie par la loi n° 82-1153 du 30 décembre 1982 d'orientation des transports intérieurs sont supprimés ;

« 5° Pour son application à Mayotte, dans le VI de l'article 10, les mots : "et L. 120-2, L. 121-8 et L. 432-2-1 du code du travail sont remplacés par les mots : "et L. 442-6 du code du travail applicable à Mayotte ;

« 6° Pour son application dans les îles Wallis et Futuna, dans le VI de l'article 10, la référence aux articles L. 120-2, L. 121-8 et L. 432-2-1 du code du travail est remplacée par la référence aux dispositions correspondantes applicables localement. »

Article 28

I. - Sous réserve des modifications prévues au 1° du III, les dispositions de la présente loi, à l'exception de l'article 3, sont applicables à Mayotte.

Sous réserve des modifications prévues au II et au 4° du III, les dispositions de la présente loi, à l'exception des articles 3, 25 et 31, sont applicables dans les îles Wallis et Futuna.

Sous réserve des modifications prévues au II et aux 2° et 3° du III, les dispositions de la présente loi, à l'exception des articles 3, 20, 25, 29 et 31, sont applicables en Nouvelle-Calédonie, en Polynésie française et dans les Terres australes et antarctiques françaises.

II. - Pour l'application de l'article 6 de la présente loi et de l'article 421-6 du code pénal, le montant des amendes en euros est remplacé par sa contre-valeur en monnaie locale en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna.

III. - Au livre VII du code monétaire et financier :

1° Pour son application à Mayotte l'article L. 735-13 est ainsi modifié :

a) Dans le premier alinéa, le mot et la référence : « et L. 574-2 » sont remplacés par le mot et la référence : « à L. 574-3 » ;

b) Au début du second alinéa, les mots : « Les références à l'article 415 du code des douanes » sont remplacés par les mots : « Les références aux articles 415 et 453 à 459 ainsi qu'aux titres II et XII du code des douanes » ;

2° Pour son application à la Nouvelle-Calédonie l'article L. 745-13 est ainsi modifié :

a) Dans le premier alinéa, le mot et la référence : « et L. 574-2 » sont remplacés par le mot et la référence : « à L. 574-3 » ;

b) Au début du second alinéa, les mots : « Les références à l'article 415 du code des douanes » sont remplacés par les mots : « Les références aux articles 415 et 453 à 459 ainsi qu'aux titres II et XII du code des douanes » ;

3° Pour son application à la Polynésie française l'article L. 755-13 est ainsi modifié :

a) Dans le premier alinéa, le mot et la référence : « et L. 574-2 » sont remplacés par le mot et la référence : « à L. 574-3 » ;

b) Au début du second alinéa, les mots : « Les références à l'article 415 du code des douanes » sont remplacés par les mots : « Les références aux articles 415 et 453 à 459 ainsi qu'aux titres II et XII du code des douanes » ;

4° Pour son application aux îles Wallis et Futuna l'article

L. 765-13 est ainsi modifié :

a) Dans le premier alinéa, le mot et la référence : « et L. 574-2 » sont remplacés par le mot et la référence : « à L. 574-3 » ;

b) Au début du second alinéa, les mots : « Les références à l'article 415 du code des douanes » sont remplacés par les mots : « Les références aux articles 415 et 453 à 459 ainsi qu'aux titres II et XII du code des douanes ».

IV. - Après l'article L. 422-5 du code des assurances, il est inséré un article L. 422-6 ainsi rédigé :

« Art. L. 422-6. - Les articles L. 422-1 à L. 422-5 sont applicables à Mayotte et dans les îles Wallis et Futuna. »

Chapitre XI

Dispositions finales

Article 29

I. - L'article L. 126-2 du code des assurances est ainsi rédigé :

« Art. L. 126-2. - Les contrats d'assurance garantissant les dommages d'incendie à des biens situés sur le territoire national ainsi que les dommages aux corps de véhicules terrestres à moteur ouvrent droit à la garantie de l'assuré pour les dommages matériels directs causés aux biens assurés par un attentat ou un acte de terrorisme tel que défini par les articles 421-1 et 421-2 du code pénal subis sur le territoire national.

« La réparation des dommages matériels, y compris les frais de décontamination, et la réparation des dommages immatériels consécutifs à ces dommages sont couvertes dans les limites de franchise et de plafond fixées au contrat au titre de la garantie incendie.

« Lorsqu'il est nécessaire de décontaminer un bien immobilier, l'indemnisation des dommages, y compris les frais de décontamination, ne peut excéder la valeur vénale de l'immeuble ou le montant des capitaux assurés.

« En outre, si l'assuré est couvert contre les pertes d'exploitation, cette garantie est étendue aux dommages causés par les attentats et les actes de terrorisme, dans les conditions prévues au contrat.

« La décontamination des déblais ainsi que leur confinement ne rentrent pas dans le champ d'application de cette garantie.

« Toute clause contraire est réputée non écrite.

« Un décret en Conseil d'Etat détermine les dérogations ou les exclusions éventuellement applicables aux contrats concernant les grands risques définis à l'article L. 111-6 au regard de l'assurabilité de ces risques. »

II. - Après l'article L. 126-2 du même code, il est inséré un article L. 126-3 ainsi rédigé :

« Art. L. 126-3. - Les entreprises d'assurance doivent insérer dans les contrats mentionnés à l'article L. 126-2 une clause étendant leur garantie aux dommages mentionnés audit article. »

III. - 1. Le I s'applique aux contrats en cours à compter de la publication de la présente loi.

2. Le II s'applique aux contrats souscrits six mois à compter de la publication de la présente loi et, pour les autres contrats, lors de la conclusion du premier avenant consécutif à l'échéance de ce même délai.

Article 30

Dans l'article 39 sexies de la loi du 29 juillet 1881 sur la liberté de la presse, les mots : « de militaires de la gendarmerie nationale » sont remplacés par les mots : « de militaires ou de personnels civils du ministère de la défense ».

Article 31

Après l'article 42-11 de la loi n° 84-610 du 16 juillet 1984 relative à l'organisation et à la promotion des activités physiques et sportives, il est inséré un article 42-12 ainsi rédigé :

« Art. 42-12. - Lorsque, par son comportement d'ensemble à l'occasion de manifestations sportives, une personne constitue une menace pour l'ordre public, le représentant de l'Etat dans le département et, à Paris, le préfet de police peuvent, par arrêté motivé, prononcer à son encontre une mesure d'interdiction de pénétrer ou de se rendre aux abords des enceintes où de telles manifestations se déroulent ou sont retransmises en public.

« L'arrêté, valable sur le territoire national, fixe le type de manifestations sportives concernées. Il ne peut excéder une durée de trois mois.

« Le représentant de l'Etat dans le département et, à Paris, le préfet de police peuvent également imposer, par le même arrêté, à la personne faisant l'objet de cette mesure l'obligation de répondre, au moment des manifestations sportives objet de l'interdiction, aux convocations de toute autorité ou de toute personne qualifiée qu'il désigne.

« Le fait, pour la personne, de ne pas se conformer à l'un ou à l'autre des arrêtés pris en application des alinéas précédents est puni de 3 750 EUR d'amende.

« Un décret en Conseil d'Etat fixe les modalités d'application du présent article. »

Article 32

Les dispositions des articles 3, 6 et 9 sont applicables jusqu'au 31 décembre 2008.

Le Gouvernement remet chaque année au Parlement un rapport sur l'application de la présente loi.

Article 33

Un arrêté interministériel détermine les services de police et de gendarmerie nationales spécialement chargés de la prévention et de la répression des actes de terrorisme au sens de la présente loi.

La présente loi sera exécutée comme loi de l'Etat.

Fait à Paris, le 23 janvier 2006.



INFORMATIQUE ET LIBERTÉS, VIE PRIVÉE

RECOMMANDATION DE LA CNIL SUR LES SITES WEB DES PARTICULIERS

Par M. Vincent DOMNESQUE,
Juriste TIC - BRM Avocats

La délibération n° 2005-285 du 22 novembre 2005, expose les recommandations de la Cnil relatives à la mise en œuvre par les particuliers de sites web diffusant ou collectant des données à caractère personnel dans le cadre d'une activité exclusivement personnelle

Parue au Journal Officiel du 17 décembre 2005, la délibération n° 2005-285 du 22 novembre 2005¹, expose les recommandations de la Cnil relatives à la mise en œuvre par les particuliers de sites web diffusant ou collectant des données à caractère personnel dans le cadre d'une activité exclusivement personnelle.

La Commission nationale de l'informatique et des libertés (Cnil) a en effet constaté un développement considérable des sites web réalisés par les particuliers. Ces sites sont le plus souvent destinés à faire partager des idées, des loisirs, une passion, ou simplement des photographies avec sa famille, ses proches ou ses amis. La recommandation concerne l'ensemble des sites créés à titre privé, et en particulier les « blogs », pour lesquels une étude Médiamétrie estime qu'un internaute sur dix a déjà créé le sien.²

Faisant application de l'article 24 de la loi du 6 janvier 1978 modifiée, la Cnil a décidé de « dispenser de déclaration les sites mis en œuvre par des particuliers dans le cadre d'une activité privée diffusant ou collectant des données à caractère personnel » (délibération n° 2005-284 du 22 novembre 2005). Cependant, s'ils permettent la collecte ou la diffusion de données à caractère personnel (nom, photographie ou tout élément permettant d'identifier une personne physique), ces sites

sont néanmoins soumis au respect des dispositions de la loi « informatique et libertés » du 6 janvier 1978.

La Cnil a donc souhaité en rappeler les règles essentielles.

Ainsi, la Commission appelle au respect du principe du consentement préalable des personnes. Il s'agit notamment d'obtenir l'accord d'une personne avant de publier sa photographie. Plus généralement, la Cnil souhaite que les personnes soient préalablement informées de l'identité du responsable du traitement, de la finalité poursuivie, de l'objet du site procédant à cette diffusion, des destinataires ou de la catégorie des destinataires des données ainsi que de l'existence d'un droit d'accès, de rectification et d'opposition. Au demeurant, la Commission recommande la plus grande discrétion sur les données faisant apparaître les opinions politiques, religieuses, philosophiques, l'appartenance ethnique, etc. au vu des risques de réutilisation et de déformation de ces données au moyen de l'outil Internet.

La Commission souligne enfin que la durée de conservation de ces données doit être en relation avec l'objet du site et que « tout transfert des données collectées ne peut s'effectuer que dans le cadre d'activités privées, après que la personne concernée en a été informée et a été mise en mesure de s'y opposer ».

Par M. Vincent DOMNESQUE,
Juriste TIC - BRM Avocats

NOTES

¹ C.N.I.L., délibération n° 2005-284 du 22 novembre 2005 décidant la dispense de déclaration des sites web diffusant ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'une activité exclusivement personnelle (norme d'exonération n° 6), J.O n° 293 du 17 décembre 2005, texte n° 79.

² Baptiste RUBAT du MERAC, *Un internaute sur dix a déjà créé un blog*, JDN, 19 décembre 2005.

NOMS DE DOMAINE, PROPRIÉTÉS INDUSTRIELLES ET COMMERCIALES

LE WHOIS DU .EU MIS EN ATTENTE

Par M. Jean-François Poussard
Rédacteur en Chef
MailClub.info

L'Eurid (la « registry » du .eu) indique que son whois (www.whois.eu) ne sera pas actualisé durant quelques jours

La première date limite pour retourner les documents justificatifs du .eu s'est finie hier, 16 janvier 2006 pour les demandes du 7 décembre 2005. L'Eurid (la « registry » du .eu) indique que son whois (www.whois.eu) ne sera pas actualisé durant quelques jours. Découvrez les conséquences de ce nouveau délai.

Trop de justificatifs entrant

L'Eurid indique que le champ réservé à la date de réception des documents n'est pas correctement mise à jour. Elle explique ce délai par l'arrivée tardive et massive des preuves justificatives. Elle demande aux candidats de .eu de prendre leur mal en patience et de re-consulter le site whois.eu d'ici quelques jours.

Six jours de retard

En consultant le whois du .eu, ce dernier indique que le champ date de réception des documents n'a pas été mis à jour depuis le 11 janvier 2006.

En attendant, de nombreux noms de domaine ont donc toujours un statut « initial » sur la base de données en ligne, alors que la date d'expiration des demandes est

dépassée. Pour ceux qui n'ont pas renvoyé leurs documents, le statut « expiré » sera mentionné dans les prochains jours.

Pour rappel, la base de données whois permet aux internautes de connaître :

- * la position de leur demande en .eu
- * la date et l'heure précise à laquelle a été soumise la demande
- * le nom du candidat
- * les coordonnées du demandeur : droit revendiqué, adresse postale, « registrar »...
- * le statut du nom de domaine : initial, accepté, rejeté, activé, non considéré
- * la date de réception des documents
- * la date limite de renvoi des justificatifs
- * la date d'activation
- * les ADR (Alternative Dispute Resolution).

Un appel entendu ?

Le 11 janvier, l'Eurid avait fait part de son inquiétude dans un communiqué. Elle s'affolait devant le peu de justificatifs reçus de la part des demandeurs de noms de domaine .eu. Il lui manquait plus de 50 000 documents, soit 50 % des demandes, à 5 jours de la date d'expiration.

L'afflux massif de documents auprès de l'agent de validation PricewaterhouseCoopers Belgique (PWC) semble démontrer que les différents interlocuteurs (« registrar », clients finaux...) se soient réveillés.

15 000 noms de domaine expirés ?

Sur la [page des statuts de l'Eurid](#), la « registry » indique avoir reçu 85 000 documents, soit 35 000 nouveaux justificatifs en 5 jours. Sur les 100 000 demandes de la première journée, 15 % n'auraient donc pas de preuves de droits antérieurs et seront donc logiquement expirés dans les jours à venir. La demande suivante sera alors étudiée par l'agent de validation.

Selon les offres commerciales des centaines de « registrar », la gestion de l'envoi des justificatifs est

prise en charge soit par le demandeur ou soit par le « registrar ». Il semble que de nombreux prestataires n'ont pas intégré l'exigence de l'Eurid et de PWC pour cette « sunrise period » du .eu.

Les commandes en « Sunrise 1 + » faites au « registrar » officiel du .eu, [MailClub](#), prennent en charge la gestion des preuves justificatives. Elles permettent au [MailClub](#) d'avoir déjà retourné 100 % des documents justificatifs à PWC.

Un long processus de validation

Si les documents sont reçus par l'agent de validation par PricewaterhouseCoopers Belgique (PWC), ce dernier va ensuite valider ses noms de domaine. Avant l'ouverture, PWC estimait le délai maximum de traitement des demandes entre 12 et 18 mois. Une fois validé par PWC, le nom de domaine en .eu sera en quarantaine, avant d'être enfin enregistré et utilisable sur la toile. On peut espérer que la grande majorité des .eu soient visibles au printemps 2006.

Priorité aux marques enregistrées durant 20 jours

La « sunrise 1 » dure jusqu'au 7 février 2006. Elle est strictement réservée aux marques nationales et communautaires enregistrées, aux appellations d'origine et aux noms et acronymes des organismes publics.

La seconde « sunrise period » débutera le 7 février 2006. Les demandes éligibles concerneront les détenteurs des droits de la première période auxquels viennent s'ajouter les marques usuelles mais non enregistrées, les noms commerciaux, les identificateurs d'entreprises, les noms de sociétés, les titres distinctifs d'œuvres littéraires ou artistiques.....

Enfin, le 7 avril 2006, le .eu s'ouvre à tous, sans droit au nom.

Par M. Jean-François Poussard
Rédacteur en Chef
[MailClub.info](#)

NOTES

- Les noms de domaine enregistrables sont soumis à un droit au nom très strict. Vous pouvez réserver vos noms de domaine sur le site spécial .eu du MailClub ([découvrez le, en cliquant ici](#)).
 - - * Vous pouvez pré-enregistrer vos demandes en Sunrise 2 sur le site spécial .eu du MailClub ([cliquez ici](#))
 - * Vous pouvez pré-enregistrer vos demandes en Basic + sur le site spécial .eu du MailClub ([cliquez ici](#))
-



DROIT DE LA CONSOMMATION, PROTECTION DU CONSOMMATEUR, PROTECTION DES MINEURS

L'OBLIGATION POUR LES FAI DE METTRE À DISPOSITION DES LOGICIELS DE CONTRÔLE PARENTAL

Par M. Vincent DOMNESQUE,
Juriste TIC - BRM Avocats

Au premier trimestre 2006, tous les nouveaux abonnés se verront proposer sans surcoût, un logiciel de filtrage et de contrôle parental dans leur kit de connexion Internet.

L'article 6 de la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004 dispose que « *les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens* ».

Lors de la Conférence nationale de la famille, clôturant dix mois de concertations entre les « principaux acteurs de la politique familiale » qui s'est tenue le 22 septembre 2005, le Gouvernement a souhaité que les logiciels de filtrage et de contrôle parental deviennent une **fonction intégrée** de l'accès Internet (avec une activation

automatique et non plus optionnelle comme c'est le cas aujourd'hui). Ceci, afin de protéger les mineurs des contenus choquants ou des rencontres dangereuses, et ainsi rendre plus sûr ce formidable outil de communication et d'éducation qu'est l'Internet.

Aussi, a-t-il été déposé le 9 novembre sur le bureau de l'Assemblée nationale, une proposition de loi visant à renforcer les obligations des fournisseurs d'accès Internet en matière de fourniture de logiciels de filtrage. Son article unique prévoyait une réécriture de l'article 6 de la LCEN libellé comme suite : « *Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne ont l'obligation de fournir à leurs abonnés au moins un moyen technique permettant de sélectionner ces services et d'intégrer dans les procédures d'accès à ces services au moins un moyen technique permettant d'en restreindre l'accès. Elles assurent la mise à jour régulière de ces moyens techniques* ».

C'est dans ce contexte qu'un [accord a été signé le 16 novembre 2005](#) entre le Gouvernement et les fournisseurs d'accès Internet. Ainsi au premier trimestre 2006, tous les nouveaux abonnés se verront proposer sans surcoût, un logiciel de filtrage et de contrôle parental dans leur kit de connexion Internet. Afin de sensibiliser aux risques du web, des campagnes de communication à destination des parents et des enfants seront menées par le Gouvernement et les fournisseurs d'accès.

Par M. Vincent DOMNESQUE,
Juriste TIC - BRM Avocats



TEXTES OFFICIELS

Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique

Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique,

J.O n° 4 du 5 janvier 2006 page 174
texte n° 14.

NOR : SANX0500308D

Le Président de la République,

Sur le rapport du Premier ministre et du ministre de la santé et des solidarités,

Vu le code du patrimoine, notamment le titre Ier du livre II ;

Vu le code de la santé publique, notamment ses articles L. 1111-7, L. 1111-8 et L. 1112-1 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, notamment ses articles 21 et 24 ;

Vu le décret n° 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques ;

Vu le décret n° 97-34 du 15 janvier 1997 modifié relatif à la déconcentration des décisions administratives individuelles, notamment son article 2 ;

Vu le décret n° 97-1185 du 19 décembre 1997 modifié pris pour l'application à la ministre de l'emploi et de la solidarité du 1° de l'article 2 du décret du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;

Vu l'avis du Conseil national de l'ordre des médecins en date du 1er avril 2004 ;

Vu l'avis du Conseil national de l'ordre des chirurgiens-dentistes en date du 8 avril 2004 ;

Vu l'avis du Conseil national de l'ordre des pharmaciens en date du 11 mai 2004 ;

Vu l'avis du Conseil national de l'ordre des sages-femmes en date du 26 mai 2004 ;

Vu les avis de la Commission nationale de l'informatique et des libertés en date des 27 mai 2004 et 15 mars 2005 ;

Le Conseil d'Etat (section sociale) entendu ;

Le conseil des ministres entendu,

Décète :

Article 1

Le chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique (dispositions réglementaires) est ainsi modifié :

I. - La section unique devient la sous-section 1, intitulée « Sous-section 1 : Accès aux informations de santé à caractère personnel », au sein d'une section 1 dont le titre est ainsi rédigé :

« Section 1 «Principes généraux »

II. - Après l'article R. 1111-8, il est ajouté une sous-section 2 ainsi rédigée :

« Sous-section 2 Hébergement des données de santé à caractère personnel

« Art. R. 1111-9. - Toute personne physique ou morale souhaitant assurer l'hébergement de données de santé à caractère personnel, mentionné à l'article L. 1111-8, et bénéficier d'un agrément à ce titre doit remplir les conditions suivantes :

« 1° Offrir toutes les garanties pour l'exercice de cette activité, notamment par le recours à des personnels qualifiés en matière de sécurité et d'archivage des données et par la mise en oeuvre de solutions techniques, d'une organisation et de procédures de contrôle assurant la sécurité, la protection, la conservation et la restitution des données confiées, ainsi qu'un usage conforme à la loi ;

« 2° Définir et mettre en oeuvre une politique de confidentialité et de sécurité, destinée notamment à assurer le respect des exigences de confidentialité et de secret prévues par les articles L. 1110-4 et L. 1111-7, la protection contre les accès non autorisés ainsi que la pérennité des données, et dont la description doit être jointe au dossier d'agrément dans les conditions fixées par l'article R. 1111-14 ;

« 3° Le cas échéant, identifier son représentant sur le territoire national au sens de l'article 5 de la loi du 6 janvier 1978 ;

« 4° Individualiser dans son organisation l'activité d'hébergement et les moyens qui lui sont dédiés, ainsi que la gestion des stocks et des flux de données ;

« 5° Définir et mettre en place des dispositifs d'information sur l'activité d'hébergement à destination des personnes à l'origine du dépôt, notamment en cas de modification substantielle des conditions de réalisation de cette activité ;

« 6° Identifier les personnes en charge de l'activité d'hébergement, dont un médecin, en précisant le lien contractuel qui les lie à l'hébergeur.

« Art. R.* 1111-10. - L'agrément nécessaire à l'activité d'hébergement de données de santé à caractère personnel est délivré par le ministre chargé de la santé, qui se prononce après avis de la Commission nationale de l'informatique et des libertés et d'un comité d'agrément placé auprès de lui.

« A cet effet, la personne intéressée adresse au ministre chargé de la santé un dossier de demande d'agrément comprenant les éléments mentionnés à l'article R. 1111-12. Le ministre transmet le dossier à la Commission nationale de l'informatique et des libertés, qui apprécie les garanties présentées par le candidat à l'agrément en matière de protection des personnes à l'égard des traitements de données de santé à caractère personnel et de sécurité de ces données. La commission rend son avis dans un délai de deux mois à compter de la réception du dossier, délai pouvant être renouvelé une fois sur décision motivée de son président.

« Dès que la commission s'est prononcée ou à l'expiration du délai qui lui était imparti, elle transmet la demande d'agrément, accompagnée, le cas échéant, de son avis, au comité d'agrément mentionné au premier alinéa. Ce comité se prononce sur tous les aspects du dossier, en particulier sur les garanties d'ordre éthique, déontologique, technique, financier et économique qu'offre le candidat. Il émet son avis dans le mois qui suit la réception du dossier transmis par la Commission nationale de l'informatique et des libertés. Il peut toutefois demander un délai supplémentaire d'un mois.

« Le ministre chargé de la santé dispose, pour prendre sa décision, d'un délai de deux mois suivant l'avis du comité d'agrément. A l'issue de ce délai, son silence vaut décision de rejet.

« Art. R. 1111-11. - I. - Le comité d'agrément mentionné à l'article R. 1111-10 comprend :

« 1° Un membre de l'inspection générale des affaires sociales nommé sur proposition du chef de l'inspection générale des affaires sociales ;

« 2° Deux représentants des associations compétentes en matière de santé, agréées au niveau national dans les conditions prévues à l'article L. 1114-1 ;

« 3° Deux représentants des professions de santé, l'un nommé sur proposition du Conseil national de l'ordre des médecins et l'autre sur proposition de l'Union nationale des professions de santé ;

« 4° Trois personnalités qualifiées :

« a) Une personne choisie en raison de ses compétences dans les domaines de l'éthique et du droit ;

« b) Une personne choisie en raison de ses compétences en matière de sécurité des systèmes d'information et de nouvelles technologies ;

« c) Une personne choisie en raison de ses compétences dans le domaine économique et financier.

« Le directeur général de la santé, le directeur de l'hospitalisation et de l'organisation des soins, le directeur des Archives de France, le directeur général des entreprises et le directeur général de la concurrence, de la consommation et de la répression des fraudes, ou leurs représentants, assistent aux séances du comité avec voix consultative.

« II. - Les membres du comité d'agrément, dont celui qui, parmi eux, exercera la présidence du comité, sont nommés pour cinq ans par arrêté du ministre chargé de la santé. Leur mandat est renouvelable une fois.

« Lors de leur entrée en fonction, les membres du comité adressent au président une déclaration mentionnant toute activité personnelle ou professionnelle en rapport direct ou indirect avec les missions du comité, ainsi que les liens directs ou indirects qu'ils peuvent avoir avec tout organisme hébergeant ou susceptible d'héberger des données de santé à caractère personnel ou avec les organismes professionnels et les sociétés de conseil intervenant dans le domaine de compétence du comité. Ils s'engagent à signaler toute modification concernant cette situation.

« Ils ne peuvent siéger lorsque est examinée une affaire relative à un organisme au sein duquel ils détiennent un intérêt, exercent des fonctions ou détiennent un mandat, ou au sein duquel ils ont, au cours des dix-huit mois précédant la séance, détenu un intérêt, exercé des fonctions ou détenu un mandat.

« Des suppléants en nombre égal au nombre de titulaires sont désignés dans les mêmes conditions que ceux-ci. Un membre titulaire empêché ou intéressé par une affaire est remplacé par son suppléant.

« Le remplacement d'un membre du comité en cas de cessation de fonction en cours de mandat est réalisé dans les mêmes conditions que sa nomination et pour la durée du mandat restant à courir.

« Les fonctions de membre du comité ouvrent droit à des indemnités pour frais de déplacement et de séjour dans les conditions prévues par les dispositions législatives et réglementaires applicables aux fonctionnaires civils de l'Etat.

« III. - Le comité d'agrément ne peut délibérer que si deux tiers au moins de ses membres sont présents. Dans le cas contraire, une nouvelle séance peut se tenir sans obligation de quorum après un délai de quinze jours.

« Les avis rendus par le comité sont motivés. Ils sont pris à la majorité des voix exprimées des membres présents. En cas de partage égal des voix, celle du président est prépondérante.

« IV. - Le comité d'agrément peut être saisi par le ministre chargé de la santé de tout sujet entrant dans son domaine de compétence.

« Art. R. 1111-12. - Le dossier de demande d'agrément comprend les éléments suivants :

« 1° L'identité et l'adresse du responsable du service d'hébergement et, le cas échéant, de son représentant ; pour les personnes morales, les statuts sont produits ;

« 2° Les noms, fonctions et qualifications des opérateurs chargés de mettre en oeuvre le service, ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont accès aux données hébergées ;

« 3° L'indication des lieux dans lesquels sera réalisé l'hébergement ;

« 4° Une description du service proposé ;

« 5° Les modèles de contrats devant être conclus, en application du deuxième alinéa de l'article L. 1111-8, entre l'hébergeur de données de santé et les personnes physiques ou morales qui sont à l'origine du dépôt des données de santé à caractère personnel ; ces modèles sont établis conformément aux dispositions de l'article R. 1111-13 ;

« 6° Les dispositions prises pour assurer la sécurité des données et la garantie des secrets protégés par la loi, notamment la présentation de la politique de confidentialité et de sécurité prévue au 2° de l'article R. 1111-9 ;

« 7° Le cas échéant, l'indication du recours à des prestataires techniques externes et les contrats conclus avec eux ;

« 8° Un document présentant les comptes prévisionnels de l'activité d'hébergement et, éventuellement, les trois derniers bilans et la composition de l'actionnariat du demandeur, ainsi que, dans le cas d'une demande de renouvellement, les comptes de résultat et bilans liés à cette activité d'hébergement depuis le dernier agrément.

« L'hébergeur déjà agréé informe sans délai le ministre chargé de la santé de tout changement affectant les informations mentionnées ci-dessus et de toute interruption, temporaire ou définitive, de son activité.

« Art. R. 1111-13. - Les modèles de contrats devant être joints à la demande d'agrément, mentionnés au 5° de l'article R. 1111-12, contiennent obligatoirement au moins les clauses suivantes :

« 1° La description des prestations réalisées : contenu des services et résultats attendus ;

« 2° Lorsque le contrat est souscrit par la personne concernée par les données hébergées, la description des modalités selon lesquelles les professionnels de santé et les établissements de santé les prenant en charge et désignés par eux peuvent être autorisés à accéder à ces données ou en demander la transmission et l'indication des conditions de mise à disposition de ces données ;

« 3° Lorsque le contrat est souscrit par un professionnel de santé ou un établissement de santé, la description des modalités selon lesquelles les données hébergées sont mises à leur disposition, ainsi que les conditions de recueil de l'accord des personnes concernées par ces données s'agissant tant de leur hébergement que de leurs modalités d'accès et de transmission ;

« 4° La description des moyens mis en oeuvre par l'hébergeur pour la fourniture des services ;

« 5° La mention des indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, ainsi que de la périodicité de leur mesure ;

« 6° Les obligations de l'hébergeur à l'égard de la personne à l'origine du dépôt des données de santé à caractère personnel en cas de modifications ou d'évolutions techniques introduites par lui ;

« 7° Une information sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'hébergeur pour que ce recours assure un niveau équivalent de garantie au regard des obligations pesant sur l'activité d'hébergement ;

« 8° Une information sur les garanties permettant de couvrir toute défaillance éventuelle de l'hébergeur ;

« 9° Une présentation des prestations à la fin de l'hébergement.

« Art. R. 1111-14. - Une présentation de la politique de confidentialité et de sécurité, prévue au 2° de l'article R. 1111-9, doit être fournie à l'appui de la demande d'agrément conformément au 6° de l'article R. 1111-12. Elle comporte notamment les précisions suivantes :

« 1° En matière de respect des droits des personnes concernées par les données hébergées :

« a) Les modalités permettant de s'assurer de l'existence du consentement de l'intéressé à l'hébergement des données le concernant ;

« b) Les modalités retenues pour que l'accès aux données de santé à caractère personnel et leur transmission éventuelle n'aient lieu qu'avec l'accord des personnes concernées et par les personnes désignées par elles ;

« c) Les conditions dans lesquelles sont présentées et prises en compte les éventuelles demandes de rectification des données de santé à caractère personnel hébergées ;

« d) Les moyens mis en oeuvre pour assurer le respect des dispositions de l'article L. 1111-7 relatif à l'accès des personnes à leurs informations de santé, notamment en termes de délais et de modalités de consultation ;

« e) Les procédures de signalement des incidents graves, dont l'altération des données ou la divulgation non autorisée des données personnelles de santé ;

« f) La fourniture à la personne concernée par les données hébergées, à sa demande, de l'historique des

accès aux données et des consultations ainsi que du contenu des informations consultées et des traitements éventuellement opérés.

« 2° En matière de sécurité de l'accès aux informations :

« a) Les dispositions prises pour garantir la sécurité des accès et des transmissions des données de santé à caractère personnel vis-à-vis des établissements ou des professionnels de santé à l'origine du dépôt et des personnes concernées par ces données ;

« b) Les mesures prises en matière de contrôle des droits d'accès et de traçabilité des accès et des traitements ;

« c) Les conditions de vérification du contenu des traces des accès et des traitements afin de détecter les tentatives d'effraction ou d'accès non autorisés ;

« d) Les modalités de vérification du registre des personnes habilitées à accéder aux données hébergées tenant compte des éventuelles mises à jour ;

« e) Les procédés techniques retenus en matière d'identification et d'authentification ; en ce qui concerne les professionnels de santé, ces procédés techniques doivent avoir été agréés par le groupement d'intérêt public mentionné à l'article R. 161-54 du code de la sécurité sociale.

« 3° En matière de pérennité des données hébergées :

« a) Les procédures visant à assurer, au moment du transfert des données vers l'hébergeur, la réception sécurisée des données et l'intégrité de celles-ci, leur prise en compte dans le système d'information de l'hébergeur et le suivi de cette prise en charge ;

« b) Les modalités de prise en compte et d'enrichissement tout au long de la durée de l'hébergement, de l'ensemble des informations concernant les données depuis leur création, telles que les données permettant de les identifier et de les décrire, de les gérer, de déterminer leurs propriétés techniques et d'en assurer la traçabilité ;

« c) Les modalités de surveillance des supports en vue d'anticiper les changements technologiques et, le cas échéant, d'opérer des migrations de supports dans des conditions en garantissant la traçabilité ;

« d) Les procédures liées à la réplique des données sur différents supports informatiques en des lieux distincts ;

« e) Les conditions de mise en oeuvre d'une alerte concernant les formats d'encodage des données, destinée à avertir la personne à l'origine du dépôt en cas d'obsolescence de ce format et, éventuellement, les procédures visant à réaliser, avec l'autorisation de la personne à l'origine du dépôt, des migrations de formats des données, si ces derniers ne permettent plus d'assurer la lisibilité des informations et à assurer la traçabilité de ces migrations.

« 4° En matière d'organisation et de procédures de contrôle interne en vue d'assurer la sécurité des traitements et des données :

« a) La désignation d'un responsable sécurité et d'un responsable qualité ;

« b) La définition des missions, des pouvoirs et des obligations des personnels de l'hébergeur et de ses éventuels sous-traitants, habilités à traiter les données de santé à caractère personnel ;

« c) Les spécifications techniques des logiciels et des mécanismes de sécurité propres à garantir la confidentialité des transmissions, notamment en ce qui concerne le mode de chiffrement des flux d'information ;

« d) Les modalités retenues pour l'évaluation périodique des risques et l'audit des mesures de protection mises en place afin de garantir la sécurité des données et en vue d'apporter les modifications nécessaires en cas de détection de défaillances ;

« e) Les dispositifs de simulation régulière de défauts de fonctionnement pour vérifier l'efficacité des mécanismes destinés à garantir la continuité des services ;

« f) Les moyens mis en oeuvre pour sensibiliser et former le personnel aux mesures de protection mises en place et à leurs obligations en matière de confidentialité et de respect du secret professionnel ;

« g) Les conditions de mise en oeuvre de la sécurité physique des sites informatiques, des mesures de protection de l'infrastructure technique, notamment en termes de sécurité des réseaux, des serveurs et des postes de travail ;

« h) Les dispositions prises en ce qui concerne l'exploitation de l'infrastructure technique ;

« i) Les conditions de mise en oeuvre du plan de secours informatique comportant notamment les dispositions prises pour informer du déclenchement de ce plan les personnes physiques ou morales à l'origine du dépôt des données de santé à caractère personnel ainsi que les dispositions prises pour la reprise des activités.

« Art. R. 1111-15. - L'agrément est délivré aux hébergeurs de données de santé à caractère personnel pour une durée de trois ans.

« La demande de renouvellement doit être déposée au plus tard six mois avant le terme de la période d'agrément. Elle comprend les documents mentionnés au 8° de l'article R. 1111-12 et un récapitulatif des modifications intervenues depuis la dernière demande d'agrément en ce qui concerne les autres documents mentionnés à cet article, ainsi qu'un audit externe réalisé aux frais de l'hébergeur, attestant de la mise en oeuvre de la politique de confidentialité et de sécurité mentionnée à l'article R. 1111-14. Elle est instruite selon la même procédure que celle applicable à la demande initiale.

« Les décisions d'agrément, ainsi que le renouvellement de cet agrément, sont publiées au Bulletin officiel du ministère de la santé.

« Art. R. 1111-16. - Le ministre chargé de la santé, lorsqu'il envisage de procéder au retrait d'un agrément en application du quatrième alinéa de l'article L. 1111-8, communique à l'hébergeur intéressé, par lettre recommandée avec demande d'avis de réception, les motifs de ce projet de retrait et l'appelle à formuler ses observations, écrites ou, à sa demande, orales, dans un délai de deux mois.

« En cas de divulgation non autorisée de données de santé à caractère personnel ou de manquements graves de l'hébergeur à ses obligations mettant notamment en cause l'intégrité, la sécurité et la pérennité des données hébergées, le ministre chargé de la santé peut, à titre conservatoire, dans l'attente qu'il soit statué définitivement sur le projet de retrait d'agrément, prononcer la suspension de l'activité d'hébergement.

« La décision de retrait est notifiée à l'hébergeur intéressé, par lettre recommandée avec demande d'avis de réception. Elle met fin de plein droit à l'hébergement des données confiées à l'hébergeur et entraîne la restitution de ces données aux personnes ayant contracté avec l'hébergeur.

« Les décisions de suspension et de retrait font l'objet de la mesure de publicité prévue à l'article R. 1111-15. Elles sont transmises pour information au comité d'agrément mentionné à l'article R. 1111-10 ainsi qu'à la Commission nationale de l'informatique et des libertés. »

Article 2

I. - Après le premier alinéa de l'article R. 1111-2 du code de la santé publique, il est inséré un alinéa ainsi rédigé :

« Dans le cas où les informations demandées sont détenues par un établissement de santé et si les dispositifs techniques de l'établissement le permettent, le demandeur peut également consulter par voie électronique tout ou partie des informations en cause. »

II. - L'article R. 1112-7 du même code est remplacé par les dispositions suivantes :

« Art. R. 1112-7. - Les informations concernant la santé des patients sont soit conservées au sein des établissements de santé qui les ont constituées, soit déposées par ces établissements auprès d'un hébergeur agréé en application des dispositions à l'article L. 1111-8.

« Le directeur de l'établissement veille à ce que toutes dispositions soient prises pour assurer la garde et la confidentialité des informations ainsi conservées ou hébergées.

« Le dossier médical mentionné à l'article R. 1112-2 est conservé pendant une durée de vingt ans à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein. Lorsqu'en application des dispositions qui précèdent, la durée de conservation d'un dossier s'achève avant le vingt-huitième anniversaire de son titulaire, la conservation du dossier est prorogée jusqu'à cette date. Dans tous les cas, si la personne titulaire du dossier décède moins de dix ans après son dernier passage dans l'établissement, le dossier est conservé pendant une durée de dix ans à compter de la date du décès. Ces délais sont suspendus par l'introduction de tout recours gracieux ou contentieux tendant à mettre en cause la responsabilité médicale de l'établissement de santé ou de professionnels de santé à raison de leurs interventions au sein de l'établissement.

« A l'issue du délai de conservation mentionné à l'alinéa précédent et après, le cas échéant, restitution à l'établissement de santé des données ayant fait l'objet d'un hébergement en application de l'article L. 1111-8, le dossier médical peut être éliminé. La décision d'élimination est prise par le directeur de l'établissement après avis du médecin responsable de l'information médicale. Dans les établissements publics de santé et les établissements de santé privés participant à l'exécution du service public hospitalier, cette élimination est en outre subordonnée au visa de l'administration des archives, qui détermine ceux de ces dossiers dont elle entend assurer la conservation indéfinie pour des raisons d'intérêt scientifique, statistique ou historique. »

III. - Le délai de conservation des dossiers médicaux fixé à l'article R. 1112-7 du code de la santé publique s'appliquera à l'issue d'un délai de douze mois suivant la publication du présent décret.

Article 3

Au 2 du titre II de l'annexe au décret n° 97-1185 du 19 décembre 1997, le tableau intitulé « code de la santé publique » est ainsi complété :

Vous pouvez consulter le tableau dans le JO n° 4 du 05/01/2006 texte numéro 14

Article 4

Les dispositions du présent décret peuvent être modifiées par décret en Conseil d'Etat, à l'exception de celles qui déterminent la compétence du ministre chargé de la santé figurant à l'article R.* 1111-10 du code de la santé publique et de celles de l'article 3 du présent décret dont la modification ne peut intervenir que dans les conditions prévues à l'article 2 du décret du 15 janvier 1997.

Article 5

Le Premier ministre, le ministre de la santé et des solidarités et le ministre de la culture et de la communication sont responsables, chacun en ce qui le concerne, de l'application du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 4 janvier 2006.



JURISPRUDENCES

**TGI VANNES, 13 juillet 2005,
UNIVERSITÉ DE BRETAGNE SUD /
M. A ET ALII**

Thèmes

Droit pénal, responsabilité

Abstract

Droit pénal, intrusion frauduleuse dans un système automatisé de traitement des données (oui), usurpation d'identité, art. L. 323-1 du Code pénal, cheval de troie, décryptage, intention délictueuse (oui), délit continu (oui), responsabilité pénale (oui)

Résumé

Des étudiants sont reconnus coupable d'intrusion frauduleuse dans un système automatisé de traitement des données après avoir usurpé l'identité des titulaires de comptes d'utilisateurs du réseau pédagogique de l'Institut Universitaire de VANNES.

Décision

TGI Vannes, 13 juillet 2005, Université de Bretagne Sud / M. A et alii

N° de jugement : 1148/2005

(Extraits)

Monsieur A. (...), ASSISTÉ DE Maître LAMON, Avocat au Barreau de RENNES, prévenu de :

(01619) ACCES FRAUDULEUX DANS UN SYSTEME DE TRAITEMENT AUTOMATISE DE DONNEES ;

FOURNITURE DE MATERIEL OU PROGRAMME INFORMATIQUE, CONCUS POUR ACCEDER FRAUDULEUSEMENT À UN SYSTEME DE TRAITEMENT AUTOMATISE DE DONNEES ;

Monsieur B. prévenu de :

(01619) ACCES FRAUDULEUX DANS UN SYSTEME DE TRAITEMENT AUTOMATISE DE DONNEES ;

Monsieur C. prévenu de :

(01619) ACCES FRAUDULEUX DANS UN SYSTEME DE TRAITEMENT AUTOMATISE DE DONNEES ;

Monsieur D. prévenu de :

(01619) ACCES FRAUDULEUX DANS UN SYSTEME DE TRAITEMENT AUTOMATISE DE DONNEES ;

(...)

Attendu que Monsieur A. est prévenu d'avoir à VANNES (56) courant octobre, novembre et jusqu'au 8 décembre 2004 accédé ou s'être maintenu frauduleusement sur tout ou partie d'un système de traitement automatisé de données en l'espèce en s'introduisant sur les comptes utilisateurs du réseau pédagogique de l'Institut Universitaire de VANNES ;

Faits prévus et réprimés par les articles 323-1, 323-5, 323-7 du codé pénal ;

D'avoir à VANNES et sur le territoire national, courant 2004 et jusqu'au 8 décembre 2004, sans motifs légitimes, détenu, offert, cédé, ou mis à disposition un équipement, un instrument, un programme informatique ou toute données, conçu ou spécialement adapté pour accéder ou se maintenir frauduleusement dans un système automatisé de données, entraver ou fausser le fonctionnement d'un système automatisé de données, introduire frauduleusement des données (...).

Attendu que Monsieur B. est prévenu d'avoir à VANNES (56) courant octobre, novembre et jusqu'au 8 décembre 2004 accédé ou s'être maintenu frauduleusement sur tout ou partie d'un système de traitement automatisé de données en l'espèce en s'introduisant sur les comptes utilisateurs du réseau pédagogique de l'Institut Universitaire de VANNES ;

Infraction prévue et réprimée par les articles 323-1, 323-5, 323-7 du codé pénal ;

Attendu que Monsieur C. est prévenu d'avoir à VANNES (56) courant octobre, novembre et jusqu'au 8 décembre 2004 accédé ou s'être maintenu frauduleusement sur tout ou partie d'un système de traitement automatisé de données en l'espèce en s'introduisant sur les comptes utilisateurs du réseau pédagogique de l'Institut Universitaire de VANNES ;

Infraction prévue et réprimée par les articles 323-1, 323-5, 323-7 du codé pénal ;

Attendu que Monsieur D. est prévenu d'avoir à VANNES (56) courant octobre, novembre et jusqu'au 8 décembre 2004 accédé ou s'être maintenu frauduleusement sur tout ou partie d'un système de traitement automatisé de données en l'espèce en s'introduisant sur les comptes utilisateurs du réseau pédagogique de l'Institut Universitaire de VANNES ;

Infraction prévue et réprimée par les articles 323-1, 323-5, 323-7 du codé pénal ;

(...)

1. L'examen des incidents de procédure

(...)

A. Sur la procédure de flagrant délit

(...) En tout état de cause, le **délit de détention d'un logiciel malveillant** reproché à Monsieur A., **infraction de nature continue**, expressément mentionné dans la plainte de l'administration autorisait le recours à la procédure de flagrant délit.

L'exception de nullité de la procédure d'enquête sera pour ces motifs écartée.

(...)

B. La nullité de la citation délivrée à A. relative à l'infraction visée par l'article 323-1-1 du Code pénal

(...) Comme le soutient à juste titre A., cette citation n'est qu'un inventaire abstrait des différentes infractions qui lui sont reprochées sans qu'il soit possible de savoir quel est le mode de commission de l'infraction (...), l'identité de celui-ci, ainsi que les opérations malveillantes pouvant être effectuées par ce logiciel.

2. L'accès frauduleux à un système de traitement automatisé de données

(...) Les investigations menées par les enquêteurs à compter du 8 décembre 2004 ont permis d'établir que les quatre prévenus, sans concertation préalable, ont téléchargé sur le réseau Internet un logiciel de décryptage des mots de passe appelé « John the ripper », ont accédé ensuite à la base de données regroupant les identifiants et les mots de passe cryptés, puis ont décryptés à l'aide de ce logiciel des mots de passe pour enfin accéder à certains comptes utilisateurs.

(...) Aucune plainte n'a été déposée pour altération ou modification des données contenues dans les comptes utilisateurs ainsi visités. Aucun élément ne permet de conclure à l'existence de tels faits.

Selon l'article 323-1 du Code pénal, le fait d'accéder ou de se maintenir, frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni

de deux ans d'emprisonnement et de 30 000 euros d'amende.

En d'autres termes, l'infraction est constituée dès lors qu'une personne, non habilitée, pénètre dans ce système tout en sachant être dépourvue d'autorisation, peu importe le mobile.

(...) Dans leurs déclarations aux services de police, les quatre prévenus ont reconnu connaître le caractère illicite d'une telle introduction. Ils ont par ailleurs signé au début de l'année universitaire une carte de bon usage des ressources informatiques (...) qui n'est que la reproduction des dispositions de l'article 323-1 du Code pénal servant de support aux poursuites.

Les quatre prévenus seront donc déclarés en conséquence coupables des faits qui leur sont reprochés.

Étudiants âgés de 18 à 20 ans au moment des faits, jamais condamnés avant ces faits qui s'inscrivent dans une attitude de défi sous une forme technologique propre à la jeunesse sans conséquence préjudiciables pour les comptes d'utilisateurs usurpés, les quatre prévenus doivent être sanctionnés par une peine d'avertissement prenant la forme d'une peine d'amende avec sursis.

Cette condamnation sera exclue du bulletin n° 2 de leur casier judiciaire afin de ne pas entraver le déroulement de leur future vie professionnelle.

Sur l'action civile

L'Université de BRETAGNE SUD (...) ne demande pas dommages et intérêts.

La minute complète du jugement sur DROIT-TIC

Référence : Tribunal de Grande Instance de Vannes, jugement du 13 juillet 2005, *UNIVERSITÉ DE BRETAGNE SUD / M. A ET ALII*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=62
