N° 2000

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 4 juin 2014.

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE SUR LA PROPOSITION DE LOI (n° 1907) DE MM. Guillaume LARRIVÉ, Éric CIOTTI, Philippe GOUJON et Olivier MARLEIX *renforçant la* ***lutte*** *contre l'****apologie*** *du* ***terrorisme*** *sur* ***internet***,

PAR M. GUILLAUME LARRIVÉ
Député

SOMMAIRE

___

Pages

MESDAMES, MESSIEURS,

Les menaces terroristes qui pèsent sur notre pays sont une réalité renouvelée que chacun, hélas, a aujourd'hui à l'esprit. Ces menaces font écho au désordre du monde. Elles mettent en péril les intérêts fondamentaux de notre nation. Elles appellent une réponse, opérationnelle autant que juridique, extrêmement déterminée, venant de l'ensemble des partis de gouvernement.

Si le terrorisme est une menace avec laquelle la France a malheureusement dû apprendre à vivre depuis longtemps, notre pays doit aujourd'hui faire face à un grave péril : celui du développement du **terrorisme au nom du djihad** (1).

Le phénomène n'est pas nouveau : ce sont des djihadistes qui ont été à l'origine de tous les projets d'attentats majeurs ayant visé la France depuis une quinzaine d'années, qu'il s'agisse du marché de Noël à Strasbourg en 2000, de l'ambassade des États-Unis en 2001, du projet d'attaque chimique à Paris en 2002 ou contre la tour Eiffel et la cathédrale Notre-Dame en 2010 (2).

Le phénomène n'est pas propre à la France : plusieurs autres pays européens servent de terre de recrutement de djihadistes, qui, ces derniers mois, rejoignent principalement la Syrie. En janvier 2014, la Commission européenne a d'ailleurs appelé les États membres de l'Union européenne à intensifier leurs efforts dans la lutte contre la radicalisation et l'extrémisme (3). Le 8 mai dernier, les ministres de l'Intérieur de neuf pays européens se sont rencontrés à Bruxelles pour renforcer la coopération des polices nationales et des services de renseignement dans la lutte contre les filières djihadistes – réunion à laquelle ont été associés le Maroc, la Tunisie, la Jordanie, les États-Unis et la Turquie.

---

(1) Notion polysémique et au contenu évolutif, le djihad est défini par le Robert *comme une guerre sainte menée pour propager et défendre l'islam.*

(2) Marc Trévidic, Jean-Charles Brisard et Thibault de Montbrial, « Agir contre le djihadisme et ses ressorts », Le Figaro, *25 avril 2014, p. 15.*

(3) Communication du 15 janvier 2014, « Prévenir la radicalisation conduisant au terrorisme et à l'extrémisme violent : renforcer l'action de l'Union européenne », COM(2013) 941 final. Celle-ci rappelle l'existence, depuis 2011, du Réseau de sensibilisation à la radicalisation (RSR), chargé de fournir des éléments d'expertise sur ces phénomènes.

S'il n'est ni nouveau ni spécifique à la France, **le développement du djihadisme violent dans notre pays s'est fortement accentué ces derniers mois, ce qui est particulièrement inquiétant**. Les Français représenteraient le premier contingent des quelque 2 000 djihadistes européens combattant en Syrie. Selon le ministre de l'Intérieur, M. Bernard Cazeneuve, les départs vers la Syrie connaissent « *une hausse accélérée et préoccupante depuis plusieurs mois. Sur un total de plus de 740 personnes détectées comme appartenant à ces filières, près de 300 se trouvent en Syrie, 130 en transit et 130 sont de retour après un ou plusieurs séjours* » [(1)].

Dans ce contexte, **internet joue un rôle essentiel, sinon décisif, dans nombre de trajectoires d'individus basculant dans la violence terroriste**, au terme de processus d'endoctrinement qui le disputent au lavage de cerveau. Comme l'a notamment souligné M. Marc Trévidic, juge d'instruction au pôle anti-terroriste du tribunal de grande instance de Paris, « *l'appel au djihad s'est affranchi des mosquées salafistes et des imams radicaux pour proliférer sur internet, où le Googlistan fait plus d'adeptes que n'importe quel prêcheur de haine* » [(2)]. Formidable outil de liberté, internet peut aussi se révéler un redoutable vecteur de propagande, de radicalisation et de recrutement pour le terrorisme.

C'est en vue de faire face à cette situation que **la proposition de loi renforçant la lutte contre l'apologie du terrorisme sur internet** (n° 1907) a été présentée par MM. Éric Ciotti, Philippe Goujon, Olivier Marleix et le signataire de ces lignes. À la demande du groupe UMP, elle a été inscrite à l'ordre du jour de la séance publique du 12 juin 2014.

Sans naturellement prétendre embrasser toute la problématique de la prévention et de la répression du terrorisme, cette proposition de loi vise à **doter notre arsenal juridique d'outils nouveaux, adaptés à l'évolution récente des menaces et, en particulier, au développement du cyberdjihadisme** :

– elle ouvre la possibilité, pour les services du ministère de l'Intérieur, d'obtenir le blocage de l'accès à certains sites internet faisant l'apologie du terrorisme ;

– elle crée un nouveau délit réprimant la consultation habituelle de sites internet incitant au terrorisme au moyen d'images montrant des atteintes volontaires à la vie commises à des fins terroristes ;

– elle élargit les moyens d'investigation des policiers et des forces de renseignement, afin de permettre à des « cyberpatrouilleurs » de constater ce nouveau délit.

---

(1) Communication en conseil des ministres du 23 avril 2014.

(2) Marc Trévidic, Jean-Charles Brisard et Thibault de Montbrial, ibid.

Ces mesures ont déjà été proposées, par deux fois, en 2012 (1). Elles n'ont malheureusement pas prospéré, faute d'abord de pouvoir être inscrites à l'ordre du jour du Parlement, en raison des élections présidentielle et législatives, puis du fait des hésitations et des réticences du Gouvernement de M. Jean-Marc Ayrault. Face à une montée des périls de plus en plus avérée, ces velléités n'ont désormais plus lieu d'être : **il est urgent d'adapter notre législation anti-terroriste aux nouvelles menaces**.

(1) Dans le projet de loi renforçant la prévention et la répression du terrorisme (n° 4497) déposé à l'Assemblée nationale, en avril 2012, par le ministre de la Justice, M. Michel Mercier, puis sous forme d'amendements au projet de loi relatif à la sécurité et à la lutte contre le terrorisme présentés, en novembre 2012, par MM. Éric Ciotti, Philippe Goujon, Olivier Marleix et le signataire de ces lignes. Voir infra.

I. INTERNET EST DEVENU LE PREMIER VECTEUR DE LA PROPAGANDE DJIHADISTE ET LE PRINCIPAL MOYEN DE RECRUTEMENT DE TERRORISTES

Si la notion de « cyberterrorisme » est parfois utilisée pour désigner la commission d'attentats sous forme *numérique* – ce que répriment les articles 323-1 et suivants du code pénal, relatifs aux atteintes aux systèmes de traitement automatisé de données [(1)] –, ce sont des attentats, des explosions et des assassinats bien *réels* qu'internet peut aussi permettre de préparer et d'organiser.

Les pratiques constatées ces dernières années, en France comme ailleurs, révèlent qu'**internet peut servir à des multiples usages et fournir de nombreuses ressources à finalité terroriste, l'ensemble formant ce que l'on peut désigner comme le « cyberdjihadisme »** :

– la diffusion de la propagande djihadiste ;

– l'endoctrinement d'esprits faibles ;

– la radicalisation par des discours de haine, parfois accompagnés d'images odieuses [(2)] ;

– le recrutement de jeunes en vue d'actions terroristes ;

– la communication discrète, bien adaptée aux stratégies de dissimulation (*taqiya*) mises en œuvre par certains terroristes ;

– la fourniture de modes d'emploi logistiques, décrivant par exemple la fabrication d'engins explosifs.

Comme l'a souligné Mme Myriam Quéméneur, magistrate, « *pour leurs besoins de propagande, de recrutement, de formation à distance ou de transmission de messages, les terroristes utilisent toutes les ressources d'internet, des espaces ouverts aux espaces protégés. Les services les plus récents fournis par le réseau peuvent même les aider à améliorer leurs capacités de repérage des cibles potentielles, grâce aux données de toutes sortes, y compris géographiques, voire d'imagerie satellitaire, qui s'y trouvent en accès libre. Les réseaux sociaux*

---

*(1) Il s'agit, par exemple, d'introduire un virus ou un programme malveillant (*malware*) dans un système informatique, en vue de perturber son fonctionnement ou d'altérer ou de pirater les données qu'il contient.*

(2) À l'instar du juge Marc Trévidic, on ne retient pas ici la notion d'« autoradicalisation », jugée peu pertinente : « L'autoradicalisation, terme à la mode, est (…) vide de sens. Même s'il est seul devant un écran d'ordinateur, surfant sur le web, passant de liens en liens, comment prétendre qu'un individu puisse s'autoradicaliser ? Comme s'il n'y avait personne de l'autre côté de l'écran, personne derrière les sites islamistes ! Comme si la propagande jihadiste diffusée sur ces sites n'était pas pensée, construite, élaborée sciemment par des administrateurs, des modérateurs, des super-modérateurs ! Comme si les groupes terroristes n'avaient pas leurs rabatteurs internautes ! Ce qu'on appelle l'autoradicalisation n'est rien d'autre que la radicalisation du XXI[e] siècle *»* (Terroristes. Les sept piliers de la déraison, *Jean-Claude Lattès, 2013, p. 80-81).*

sont également une forme de lien à distance, décentralisé, favorisant l'interaction, parfaitement adaptée à un réseau terroriste. Internet, lieu d'échange pour les terroristes est devenu un vecteur de radicalisation et de recrutement pour le terrorisme d'inspiration djihadiste » [(1)].

Si quelques études isolées – telles que celle diffusée en mai 2014 par la fondation Quilliam [(2)] – s'essaient à relativiser le poids des sites internet dans les phénomènes de radicalisation extrémiste, pour ainsi mieux contester toute idée de mesures restrictives à leur égard, **la quasi-totalité des personnes auditionnées par votre rapporteur ont souligné qu'internet était aujourd'hui devenu le vecteur principal, sinon exclusif, de la propagande djihadiste et du recrutement de terroristes**.

Le chef de l'Unité de coordination de la lutte antiterroriste (UCLAT) [(3)], M. Loïc Garnier, estimait en 2013 : « *nous avons sur notre sol des dizaines de Mohamed Merah en puissance capables de passer à la vitesse supérieure en trois jours, en réalisant les recettes d'engins explosifs tirées d'*Inspire *ou d'autres sites islamistes vénéneux* » [(4)]. Entendu par votre rapporteur, M. Garnier a confirmé que **la propagation du terrorisme *via* internet était aujourd'hui la première préoccupation des services antiterroristes, estimant qu'internet était presque devenu « *incontrôlable* »**.

Il a également souligné que la plupart des individus interpellés dans des affaires de terrorisme djihadiste disposaient, sur leur ordinateur ou en version imprimée, de la **revue en ligne *Inspire***. Il s'agit d'un magazine rédigé en anglais, distribué sur internet depuis l'été 2010, édité au Yémen par AQPA (Al-Qaïda dans la péninsule arabique), avec pour finalité d'élargir au monde occidental l'ère du « djihad médiatique ».

À titre d'**exemple de ce que n'importe qui peut trouver en quelques minutes sur internet**, le numéro de printemps 2014 de la revue *Inspire* comporte notamment, dans une rubrique intitulée « *Bomb School* », **un mode d'emploi – descriptifs détaillés et photos à l'appui – de fabrication d'une bombe, en vue d'attentats à la voiture piégée aux États-Unis**. Une autre rubrique fournit **des suggestions de cibles d'attentats, en particulier en France** : dans les zones touristiques, dans les trains express régionaux, dans certains lieux parisiens, dans la vallée de la Dordogne, laquelle offrirait l'avantage, pendant l'été, de permettre de faire « d'une pierre deux coups » (« *Hit two birds with one stone* »), en assassinant à la fois des Français et des Anglais…

---

(1) « Le terrorisme face au cyberespace. De l'anticipation des risques à la répression », AJ Pénal, *2013, p. 446.*

(2) Jihad Trending : A Comprehensive Analysis of Online Extremism and How to Counter it, *mai 2014.*

(3) L'UCLAT, qui relève de la direction générale de la police nationale (DGPN), est chargée de la coordination opérationnelle des services appelés à lutter contre le terrorisme.

(4) Cité par Patricia Tourancheau dans « Le jihad nouvelle génération », Libération, *20 mai 2013.*

Également entendu par votre rapporteur, M. Patrick Calvar, directeur général de la sécurité intérieure (DGSI), a confirmé qu'**en matière de terrorisme, internet était aujourd'hui « *le problème majeur* »** : c'est parce ce biais, et non plus par la fréquentation de certaines mosquées ou par l'enrôlement dans certaines associations, que s'effectuent la propagande djihadiste et le recrutement terroriste.

Fin connaisseur de ces questions, M. Marc Trévidic, juge d'instruction au pôle anti-terroriste du tribunal de grande instance de Paris, a indiqué à votre rapporteur que la difficulté souvent posée résidait dans **le mélange, sur un même site internet, de divers contenus, les uns, parfaitement licites et anodins, côtoyant les autres, appelant au *djihad* contre l'Occident**.

Dans le même sens, M. Hassen Chalghoumi, président de la conférence des imams de France, a insisté sur **le caractère décisif d'internet dans la propagation des idées terroristes**. Internet permet ainsi d'atteindre de « nouveaux publics », citant l'exemple du départ pour le djihad en Syrie d'une jeune fille résidant dans le Val-d'Oise, apparemment bien intégrée – sa mère travaille à la préfecture –, sans jamais avoir fréquenté le moindre lieu de culte. Les dégâts causés par internet se mesurent également à la vitesse de diffusion des images qui y circulent. À titre d'illustration, une vidéo mise en ligne en février 2014 montrant le « quotidien » de jeunes djihadistes français en Syrie, comportant des scènes particulièrement choquantes, a été visionnée à plus de 980 000 reprises. **« *Si l'on parvenait à bloquer de telles vidéos, il y aurait moins de dégâts* » a souligné M. Chalghoumi** devant votre rapporteur.

Également auditionné par votre rapporteur, M. Rezk Shehata, président de l'association « Laïcité pour tous » a, quant à lui, évoqué **les risques liés au retour en France des nombreux djihadistes aujourd'hui en Syrie**, craignant un « *désastre* » semblable à celui connu par certains pays touchés par le terrorisme, tels que l'Égypte.

Au nom du Conseil représentatif des institutions juives de France (CRIF), M. Yonathan Arfi, vice-président, et M. Robert Ejnes, directeur exécutif, ont souligné devant votre rapporteur que, ces dernières années, **internet avait « *changé la donne* » en matière de diffusion des idées extrémistes** et qu'il convenait de se doter de moyens d'y faire face.

Pour s'en tenir ici à la seule question du terrorisme, on doit d'ailleurs relever que **les signalements de sites internet auprès de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) sont en nette progression**. Selon les informations recueillies par votre rapporteur auprès de Mme Valérie Maldonado, directrice de l'OCLCTIC, alors que 13 signalements de ce type avaient été enregistrés en 2011, ce nombre a été porté à 120 en 2012, puis à 360 en 2013 – soit **près d'un signalement pour apologie du terrorisme par jour**. En 2013, les principaux sites concernés par ces signalements ont été les réseaux sociaux (en particulier *Facebook* et *Twitter*), qui représentaient 54 % du total, suivis de blogs (14 %), de

sites internet thématiques (13 %), de *Youtube* (6 %), de forums (6 %) et de divers autres sites (7 %).

Face à une telle situation, **s'en remettre à l'autorégulation des réseaux serait illusoire**. Si les représentants de *Google France* entendus par votre rapporteur – M. Francis Donnat, directeur des politiques publiques, et M. Thibault Guiroy, conseiller au service juridique – ont exposé les actions entreprises par leur entreprise pour lutter contre les contenus illicites sur internet, la faible efficacité de telles actions peut se mesurer des plus facilement en constatant qu'**interrogé avec les mots « *jihad* » et « *decapitations* », le moteur de recherche de vidéos de *Google* fournit environ 274 000 résultats** (1).

II. LA RÉPONSE JURIDIQUE ET OPÉRATIONNELLE À LA MENACE TERRORISTE SUR INTERNET EST ENCORE TRÈS INSUFFISANTE

S'il existe déjà certains outils juridiques de lutte contre l'apologie du terrorisme sur internet, le Gouvernement tarde à avancer sur ce sujet – pourtant crucial et en plein développement. Cette situation est d'autant plus préoccupante que les mesures envisagées au plan de l'Union européenne restent également très velléitaires.

A. IL EXISTE CERTES DES OUTILS DE LUTTE CONTRE L'APOLOGIE DU TERRORISME SUR INTERNET, RÉCEMMENT RENFORCÉS PAR LA LOI DU 21 DÉCEMBRE 2012

Depuis 1986, une quinzaine de lois sont intervenues pour amender le dispositif juridique de prévention et de répression des actes de terrorisme : la question spécifique de la diffusion des idées terroristes et de leur apologie est loin d'être inconnue de notre droit.

L'outil privilégié en la matière est **le délit prévu au sixième alinéa de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse**, qui punit de cinq ans d'emprisonnement et de 45 000 euros d'amende ceux qui, par voie de presse ou par tout autre moyen de publication, « *auront **provoqué directement aux actes de terrorisme** prévus par le titre II du livre IV du code pénal, ou qui en auront fait **l'apologie*** ».

Pour mémoire, les actes de terrorisme en question, définis par le code pénal, peuvent être classés en deux catégories :

– *les infractions de droit commun commises en lien avec une entreprise à caractère terroriste*, c'est-à-dire commises « *intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur* » (article 421-1 du code pénal). Y figurent notamment les atteintes volontaires à la vie ou à l'intégrité des personnes,

(1) Site consulté par votre rapporteur le 28 mai 2014.

les enlèvements et séquestrations, les détournements de moyens de transport, les vols, extorsions, destructions, dégradations et détériorations, les infractions en matière informatique, les infractions en matière de groupes de combat et de mouvements dissous, les infractions liées aux armes, produits explosifs ou matières nucléaires, le blanchiment et le délit d'initié ;

– *les infractions spécifiques*, telles que le terrorisme écologique (article 421-2), l'association de malfaiteurs en relation avec une entreprise terroriste (article 421-2-1), le financement du terrorisme (article 421-2-2), la non-justification de ressources en cas de relations habituelles avec des personnes se livrant à des actes de terrorisme (article 421-2-3) ou le recrutement terroriste (article 421-2-4).

Deux types de comportement sont donc érigés en délit par la loi de 1881 précitée : la **provocation** directe au terrorisme et l'**apologie** du terrorisme.

À titre d'illustration récente, c'est sur le fondement de ces dispositions que, le 4 mars 2014, la 17e chambre du tribunal correctionnel de Paris a condamné Romain Letellier à un an de prison ferme et deux ans avec sursis pour « *apologie d'actes de terrorisme* » et « *provocation à la commission d'actes terroristes* ». Celui-ci était « modérateur » du forum *Ansar-alhaqq.net*, le deuxième plus important site de propagande djihadiste francophone, lequel avait notamment publié la traduction en français de la revue en ligne *Inspire*, précédemment évoquée.

D'autres incriminations peuvent également, en fonction des situations et des comportements, être mobilisées pour lutter contre la diffusion d'idées ou de projets terroristes. Tel est notamment le cas :

– du délit d'**association de malfaiteurs en relation avec une entreprise terroriste**, prévu à l'article 421-2-1 du code pénal. Celui-ci suppose toutefois l'existence d' « *un ou plusieurs faits matériels* » caractérisant la préparation d'un acte terroriste ;

– du délit de **diffusion de procédés permettant la fabrication d'engins explosifs**. L'article 322-6-1 du code pénal punit d'un an d'emprisonnement et de 15 000 euros d'amende le fait de diffuser des procédés permettant la fabrication d'engins de destruction élaborés à partir de poudre ou de substances explosives, de matières nucléaires, biologiques ou chimiques, ou à partir de tout autre produit destiné à l'usage domestique, industriel ou agricole. Soulignons que les peines sont portées à trois ans d'emprisonnement et à 45 000 euros d'amende lorsque la diffusion a été effectuée par l'intermédiaire d' « *un réseau de communication électronique à destination d'un public non déterminé* » – par exemple sur internet.

Sous la législature précédente, peu de temps après les tueries perpétrées à Toulouse et à Montauban par Mohamed Merah, **un projet de loi renforçant la prévention et la répression du terrorisme** (n° 4497) avait été déposé à l'Assemblée nationale, en avril 2012, à la demande du président de la République,

M. Nicolas Sarkozy, par le ministre de la Justice, M. Michel Mercier. Le Gouvernement issu des élections présidentielle et législatives de 2012 a malheureusement choisi de ne pas faire débattre le Parlement de ce projet de loi, qui comportait déjà plusieurs des dispositions figurant dans la présente proposition de loi, en particulier **la création d'un nouveau délit punissant toute personne qui consulte de manière habituelle, sans motif légitime, des sites internet qui provoquent au terrorisme ou en font l'apologie**.

Après l'alternance de 2012, le ministre de l'Intérieur, M. Manuel Valls, a présenté un nouveau projet visant à renforcer notre législation anti-terroriste, qui a abouti à **la loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme**. Celle-ci a édicté plusieurs dispositions ayant un lien avec les problématiques du djihadisme et de l'apologie du terrorisme.

Le législateur a, en effet, cherché à tenir compte de l'évolution des comportements des terroristes qui, souvent à la suite de contacts établis sur internet, partent pour des camps d'entraînement en Afghanistan, au Pakistan ou en Syrie.

C'est pour remédier à cette situation qu'a été modifié l'article 113-13 du code pénal, afin de prévoir que « *la loi pénale française s'applique aux crimes et délits qualifiés d'actes de terrorisme et réprimés par le titre II du livre IV commis à l'étranger par un Français ou par une personne résidant habituellement sur le territoire français* ». Autrement dit, **tout crime ou délit terroriste commis à l'étranger par un Français peut désormais être poursuivi en France**. Cela permet de condamner les Français qui se rendraient à l'étranger pour participer à des camps d'entraînement terroriste, sans avoir commis aucun acte terroriste sur le territoire français.

En outre, la loi du 21 décembre 2012 a apporté deux modifications à la loi du 29 juillet 1881 sur la liberté de la presse, dont l'article 24 – on l'a vu – réprime la provocation directe à des actes de terrorisme et l'apologie de tels actes.

D'une part, **cette loi autorise désormais le placement en détention provisoire** des personnes poursuivies pour provocation au terrorisme ou apologie du terrorisme – alors que, s'agissant d'un délit de presse, cette possibilité était jusqu'alors exclue (article 52 de la loi de 1881).

D'autre part, **le délai de prescription de l'action publique applicable à ces infractions a été allongé, pour être porté à un an** – au lieu de trois mois auparavant (article 65-3 de la loi de 1881).

En outre, la loi du 21 décembre 2012 a créé un nouveau **délit de recrutement terroriste**. Puni de dix années de prison et de 150 000 euros d'amende, il est défini comme le fait d'adresser à une personne des offres ou des promesses, de lui proposer des dons, présents ou avantages quelconques, de la menacer ou d'exercer sur elle des pressions, afin qu'elle participe à un groupement

ou une entente terroriste ou qu'elle commette un acte de terrorisme, même lorsque ces sollicitations n'ont pas été suivies d'effet (article 421-2-4 du code pénal).

Enfin, dans le but de lutter contre le financement du terrorisme, la loi du 21 décembre 2012 a **élargi le dispositif de gel des avoirs financiers aux personnes qui *incitent* à la commission d'actes terroristes** (article 562-1 du code monétaire et financier). Récemment, plusieurs arrêtés du ministre de l'Économie et des finances ont ainsi gelé les avoirs financiers d'individus ou d'associations diffusant des messages sur internet faisant l'apologie du terrorisme [(1)].

Votre rapporteur ne peut que saluer ces mesures, qu'il a, comme les autres députés du groupe UMP, votées au nom de l'intérêt général – conduisant à ce que l'Assemblée nationale approuve, en première lecture, le projet de loi à l'unanimité [(2)]. On doit d'ailleurs regretter que la majorité actuelle, lorsqu'elle était dans l'opposition, n'ait pas toujours fait preuve du même état d'esprit – par exemple en s'abstenant lors de l'adoption 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.

En définitive, notre législation actuelle n'est pas totalement démunie face à la diffusion des idées terroristes. Pour autant, l'on ne saurait mésestimer le caractère « *polymorphe et évolutif de la menace terroriste, face à laquelle les outils législatifs, juridiques et opérationnels doivent sans cesse être adaptés* » [(3)].

B. LE GOUVERNEMENT TARDE AUJOURD'HUI À AVANCER POUR AMÉLIORER LA LUTTE CONTRE LE CYBERDJIHADISME

Dès la discussion, le 27 novembre 2012, du projet de loi relatif à la sécurité et à la lutte contre le terrorisme, **le signataire de ces lignes avait, avec ses collègues Éric Ciotti, Nathalie Kosciusko-Morizet et Philippe Goujon, regretté que ce texte ne comporte aucune mesure permettant d'améliorer la lutte contre le cyberdjihadisme**. Plusieurs amendements avaient été proposés en ce sens, mais tous avaient été rejetés [(4)]. Le ministre de l'Intérieur de l'époque, M. Manuel Valls, avait néanmoins déclaré : « *J'imagine que nous pourrons cependant évoluer sur ces questions dans les mois ou les années qui viennent* ».

La récente détermination affichée par le Gouvernement en matière de lutte contre le djihadisme violent ne peut d'ailleurs conduire qu'à regretter que la

---

*(1) Voir par exemple les arrêtés du 23 janvier 2014 (*JO *du 28 janvier, p. 1640), du 18 mars 2014 (*JO *du 23 mars, p. 5726) et du 28 mai 2014 (*JO *du 3 juin, p. 9238) portant application des articles L. 562-1 et suivants du code monétaire et financier.*

(2) Troisième séance du 27 novembre 2012.

(3) Compagnie européenne d'intelligence stratégique (CEIS), Une nouvelle approche du terrorisme. Mieux comprendre le profil des groupes terroristes et de leurs membres*, mai 2013.*

(4) Voir les débats en séance publique lors de la troisième séance du 27 novembre 2012 et les amendements n[os] 13, 14, 16, 25 et 26 rectifié.

majorité n'ait pas souhaité donner suite, dès novembre 2012, à nos propositions – qui recoupent en partie les dernières annonces gouvernementales.

C'est ainsi que, le 23 avril 2014, le ministre de l'Intérieur, M. Bernard Cazeneuve, a présenté devant le conseil des ministres une communication relative à un **« *plan de lutte contre la radicalisation violente et les filières terroristes* »**. La semaine suivante, M. Cazeneuve a exposé les grandes lignes de ce plan devant votre commission des Lois [(1)].

Ce plan tend d'abord à limiter les déplacements des terroristes vers ou depuis la Syrie. À cette fin, devrait être prochainement présenté un projet de loi organisant un régime d'opposition à la sortie du territoire des personnes majeures engagées dans des activités terroristes.

Le Gouvernement a également annoncé une intensification de la lutte active contre les filières djihadistes : renforcement de l'action des services de renseignement, éloignement des étrangers impliqués dans ces filières, gel des avoirs des structures concernées, etc. **Deux autres mesures annoncées par le Gouvernement recoupent très largement la présente proposition de loi** : le développement des possibilités de détection des filières sur internet, par la généralisation de l'enquête sous pseudonyme ; les « *impulsions (…) en direction des grands opérateurs de l'internet* », afin que les contenus illicites et les sites de recrutement puissent être rapidement supprimés.

Le plan annoncé le 23 avril dernier prévoit, par ailleurs, d'améliorer la coopération internationale avec les autres pays de départ et les pays de transit. Il comporte, enfin, une série d'actions préventives (telles que la mise en place d'un « numéro vert » à destination des familles) et des opérations visant à « *contredire les prêcheurs de haine* ».

Votre rapporteur, comme ses collègues de l'UMP, approuve ce plan dans son principe, tout spécialement dans ses volets opérationnels. Il souligne, en particulier, la nécessité de développer les discours de prévention, visant à lutter contre la banalisation des idées extrémistes et violentes [(2)]. Tel est l'objet du réseau européen *Radicalisation Awareness Network* (RAN), auquel participe notamment l'Association française des victimes de terrorisme (AFVT), présidée par M. Guillaume Denoix de Saint Marc, que votre rapporteur a auditionné.

Pour autant, **il est nécessaire d'aller plus loin et de doter dès maintenant les enquêteurs et les différents services impliqués dans la prévention du terrorisme d'instruments législatifs supplémentaires, leur permettant de faire face au développement du cyberdjihadisme**.

S'il ne représente, bien entendu, qu'une facette de la lutte contre le terrorisme, internet constitue aujourd'hui le « *vecteur principal, pour ne pas dire*

(1) Compte rendu de la commission des Lois n° 52 du 30 avril 2014.

(2) Discours dits « contre-narratifs » dans les dispositifs adoptés par l'Union européenne.

exclusif, de la propagande », comme l'a déclaré le ministre de l'Intérieur lui-même [(1)]. **Trop longtemps repoussée, cette question mérite désormais d'être traitée au plus vite**, sans attendre le prochain projet de loi en la matière – qui, probablement présenté en conseil des ministres avant la mi-juillet, ne sera pas discuté au Parlement avant le second semestre [(2)]. Tel est précisément l'objet de la présente proposition de loi.

C. LES MESURES ENVISAGÉES AU PLAN EUROPÉEN SONT TROP VELLÉITAIRES

L'Union européenne tarde à aborder de manière efficace la problématique de l'apologie du terrorisme sur internet. Pour l'heure, on doit malheureusement regretter que **la prise en compte de ce phénomène demeure particulièrement limitée** :

– la communication précitée de la Commission européenne du 15 janvier 2014 [(3)] relève, à bien des égards, d'un catalogue de bonnes intentions à destination des États membres ;

– **les orientations définies, le 12 mai 2014, par le Conseil de l'Union européenne en matière de liberté d'expression en ligne et hors ligne** [(4)] **ne mentionnent même pas le terrorisme** parmi les motifs pouvant justifier des restrictions auprès des opérateurs internet. **C'est une carence très regrettable, qui aurait dû être soulignée par le Gouvernement français** ;

– l'actuel projet de révision de la stratégie européenne de lutte contre la radicalisation et le recrutement terroriste, qui sera prochainement soumis au Conseil, s'en tient à des mesures plus prospectives que réellement opérationnelles [(5)].

En sens inverse, votre rapporteur souligne qu'**un récent arrêt de la Cour de justice de l'Union européenne** (CJUE), dont l'objet est certes étranger à la question du terrorisme, **offre d'encourageantes perspectives en matière de responsabilisation des acteurs de l'internet** à l'égard des données qu'ils hébergent ou auxquelles ils renvoient. Dans son arrêt du 13 mai 2014, qui opposait l'Espagne à *Google*, la Cour de justice a jugé le moteur de recherche responsable du traitement qu'il effectue des données personnelles apparaissant sur des pages

---

(1) M. Bernard Cazeneuve, compte-rendu de la commission des Lois n° 52 du 30 avril 2014.

(2) Selon les indications fournies par M. Bernard Cazeneuve, compte-rendu de la commission des Lois n° 52 du 30 avril 2014.

(3) Voir supra, *introduction.*

(4) EU Human Rights Guidelines on Freedom of Expression Online and Offline, *12 mai 2014.*

(5) Par exemple : « nous devons continuer à étudier les moyens de prévenir activement la radicalisation et le recrutement terroriste par le biais d'internet et des réseaux sociaux. Nous répondrons à ces questions dans le cadre de nos dialogues politiques et nous offrirons un soutien technique en vue d'encourager les autres [États], en dehors de l'Union européenne, à faire de même » *(*Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism, *19 mai 2014, n° 9956/14, passage traduit par votre rapporteur).*

web publiées par des tiers [1]. Cette jurisprudence pourrait ouvrir à d'intéressantes évolutions des règles régissant traditionnellement internet, selon lesquelles les fournisseurs d'accès, les hébergeurs et autres prestataires techniques n'ont aujourd'hui aucune obligation d'assurer une veille des contenus mis en ligne, ni *a fortiori* de faire disparaître, de leur propre initiative, des messages ou images illicites.

III. IL Y A URGENCE À SE DOTER D'OUTILS JURIDIQUES SUPPLÉMENTAIRES, ADAPTÉS AUX NOUVELLES MENACES DU CYBERDJIHADISME

Il faut rappeler que notre pays a déjà connu des batailles juridiques victorieusement menées contre l'extrémisme. Pour ne citer qu'un seul exemple, rappelons qu'en 2004, les efforts conjugués des pouvoirs publics avaient abouti à l'interdiction de la diffusion en France, par satellite, de la chaîne libanaise *Al Manar*, en raison du caractère antisémite de certains de ses programmes. Cette interdiction n'avait été rendue possible que parce que le législateur, intervenu au cœur du « bras de fer » opposant le Conseil supérieur de l'audiovisuel (CSA) à cette chaîne, lui avait donné les moyens juridiques nécessaires [2].

Dans le même esprit, afin d'améliorer les moyens de lutte contre les « *djihadistes 2.0* », pour reprendre l'expression du criminologue Alain Bauer [3], la présente proposition de loi tend ainsi à **renforcer la lutte contre l'apologie du terrorisme sur internet**.

Adopter ces mesures apporterait **une première série d'outils permettant de combattre un phénomène dont l'ampleur et la gravité sont désormais unanimement reconnues, mais qui ne fait pourtant l'objet d'aucune véritable réponse des pouvoirs publics**.

Quatre principaux outils – proposés, comme on l'a vu, dès 2012 – sont prévus dans la présente proposition de loi :

– l'édiction d'une obligation de signalement aux autorités publiques, par les fournisseurs d'accès à internet et les hébergeurs, des sites provoquant au terrorisme ou en faisant l'apologie ;

– la faculté donnée aux pouvoirs publics d'obtenir le blocage de l'accès à certains sites internet provoquant au terrorisme ou en faisant l'apologie ;

---

(1) CJUE, 13 mai 2014, Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González, *C-131/12.*

(2) Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle. Cette loi a élargi les possibilités pour le CSA de saisir le Conseil d'État en cas de méconnaissance par une chaîne de ses obligations.

(3) Cité par Patricia Tourancheau dans « Le jihad nouvelle génération », ibid.

– la création d'un délit de consultation habituelle de certains sites provoquant au terrorisme ou comportant certaines images concourant à l'apologie d'actes terroristes ;

– l'élargissement des capacités d'action des « cyberpatrouilleurs » qui, grâce à l'usage de pseudonymes, peuvent infiltrer les sites faisant l'apologie du terrorisme.

A. LE RENFORCEMENT DES OBLIGATIONS DE SURVEILLANCE DES FOURNISSEURS D'ACCÈS À INTERNET ET DES HÉBERGEURS DE SITES

Le **1°** de l'**article 1er** de la proposition de loi tend à **élargir les obligations de surveillance pesant sur les acteurs de l'internet aux sites provoquant au terrorisme ou en faisant l'apologie**. L'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) serait modifié en ce sens.

Ainsi, **les fournisseurs d'accès à internet et les hébergeurs de sites internet seraient soumis à une triple obligation de vigilance** :

– ils devraient mettre en place un dispositif permettant à toute personne de porter à leur connaissance l'existence de sites ou de pages internet appelant à la commission d'actes terroristes ou faisant l'apologie du terrorisme ;

– ils devraient, en cas de tels signalements, en informer au plus vite les pouvoirs publics ;

– ils devraient rendre publics les moyens qu'ils consacrent à la lutte contre les sites internet provoquant au terrorisme ou en faisant l'apologie.

Les fournisseurs d'accès et les hébergeurs de sites internet sont déjà soumis à de semblables obligations à l'égard de plusieurs contenus considérés comme illicites [(1)]. On ne peut que s'étonner qu'il n'en aille pas de même en matière de terrorisme.

B. LA FACULTÉ DE BLOCAGE DE SITES INTERNET FAISANT L'APOLOGIE DU TERRORISME

Le **2°** de l'**article 1er** de la proposition de loi vise à **permettre, à la demande du ministre de l'Intérieur, le blocage de l'accès à certains sites provoquant au terrorisme ou en faisant l'apologie**.

(1) Troisième alinéa du 7 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée.

Quoique novatrice, cette mesure n'est pas inédite, puisqu'elle peut se prévaloir, depuis 2011, du précédent de la lutte contre les sites diffusant des images pornographiques de mineurs [(1)].

Concrètement, **elle permettrait aux services du ministère de l'Intérieur d'établir une « liste noire » de sites internet ou de certaines de leurs pages** – champ qui inclut les réseaux sociaux tels que *Facebook* ou *Instagram* – **dont l'accès devrait alors être bloqué par les fournisseurs d'accès à internet** (Orange, Free, Bouygues Telecom, SFR, Numericable, etc.) [(2)], au motif que ces sites font l'apologie d'actes de terrorisme réprimés par le code pénal.

Comme en matière de pédopornographie, faute de pouvoir obtenir ni la fermeture de sites hébergés pour la plupart à l'étranger, ni même le retrait des contenus jugés illicites, **le dispositif proposé permettrait au moins de bloquer l'accès à ces sites par les internautes français**. Ce dispositif va dans le sens des annonces faites par M. Bernard Cazeneuve, ministre de l'Intérieur, lors de son audition, le 30 avril 2014, par votre commission des Lois : « *nous agirons (…) auprès des opérateurs pour qu'ils "coupent" les discours, les vidéos et les images servant à l'endoctrinement* » [(3)]. Les 3 et 4 juin 2014, M. Cazeneuve ajoutait : « *il faut combattre l'accès sur internet à des vidéos, à des instruments de propagande, à des photos incitant* [des] *jeunes à basculer, car beaucoup de ces jeunes basculent dans la violence par une relation sur internet exclusive de toute autre* » ; « *nous avons l'intention de faire en sorte que nous puissions bloquer l'accès sur internet à des images ou à des vidéos susceptibles d'accompagner le basculement dans la radicalité* » [(4)].

Toutes les personnalités entendues par votre rapporteur [(5)] ont indiqué qu'**un dispositif de blocage serait de nature à fortement diminuer la visibilité des sites faisant l'apologie du terrorisme** – contre lesquels aucune mesure concrète et efficace n'est prise aujourd'hui, alors même que certaines vidéos montrant des décapitations sont régulièrement visionnées par plusieurs dizaines de milliers d'internautes.

Cette mesure de police administrative est justifiée par l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public, dont le Conseil

---

(1) Article 4 de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2), ayant introduit un cinquième alinéa au 7 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée.

(2) Les fournisseurs d'accès à internet sont définis au 1 de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée comme « les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne *».*

(3) Compte-rendu de la commission des Lois n° 52 du 30 avril 2014. Dans le même sens, la communication en conseil des ministres précitée indique : « Des impulsions seront (…) données, en France comme au niveau européen, en direction des grands opérateurs de l'internet, afin que les contenus illicites et les sites de recrutement fassent l'objet de procédures de suppression effective et rapide *».*

(4) Respectivement : première séance du 3 juin 2014 et première séance du 4 juin 2014.

(5) La liste des auditions figure en annexe du présent rapport.

constitutionnel a déjà admis – notamment en matière de pédopornographie [(1)] – qu'il pouvait justifier des limitations à la liberté de communication.

Un tel dispositif n'aboutirait pas à une interdiction *générale* de tous les sites internet diffusant ou relayant des idées terroristes. Il constituerait simplement un outil supplémentaire, souple et réactif, à la disposition des autorités chargées de lutter contre le terrorisme : c'est à elles qu'il reviendrait, si elles le jugeaient utile et pertinent, de demander le blocage de l'accès à des sites particulièrement sensibles ou spécialement dangereux.

Dès lors que ces interdictions seraient nécessairement *ciblées*, portant sur un nombre limité de sites, il n'y a pas lieu de craindre que cette mesure prive les services de renseignement de l'accès à certaines informations relatives à des individus surveillés ou à des projets terroristes [(2)].

C. UN NOUVEAU DÉLIT DE CONSULTATION HABITUELLE DE CERTAINS SITES INTERNET FAISANT L'APOLOGIE DU TERRORISME

L'**article 2** de la présente proposition de loi tend à créer **un nouveau délit de consultation habituelle de certains sites internet provoquant à des actes de terrorisme ou faisant l'apologie du terrorisme**.

Un nouvel article 421-2-4-1 serait introduit en ce sens dans le code pénal, disposant que « *le fait de consulter de façon habituelle un service de communication au public en ligne mettant à disposition des messages, soit provoquant directement à des actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ces messages comportent des images montrant la commission d'actes de terrorisme consistant en des atteintes volontaires à la vie* ».

Ces dispositions s'inspirent de l'article 227-23 du code pénal qui, depuis 2007, sanctionne la consultation habituelle de sites pédopornographiques [(3)].

Afin de respecter tant le principe de légalité des délits et des peines que la liberté de communication, le nouveau délit ici proposé ne s'appliquerait pas à

---

(1) Décision n° 2011-625 DC du 10 mars 2011, Loi d'orientation et de programmation pour la performance de la sécurité intérieure.

(2) Crainte évoquée notamment par M. Bernard Cazeneuve lors de son audition précitée : « si nous y parvenions [*i.e.* : à bloquer l'accès à des sites], les membres des réseaux djihadistes, réseaux internationaux, pourraient continuer de s'informer ailleurs tout en restant sur notre territoire, alors que nous nous priverions d'un moyen d'y détecter leur présence » *(compte rendu de la commission des Lois n° 52 du 30 avril 2014).*

(3) Loi n° 2007-293 du 5 mars 2007 réformant la protection de l'enfance.

l'ensemble des sites diffusant des idées terroristes [(1)], mais seulement à deux catégories d'entre eux [(2)] :

– les sites **« *mettant à disposition des messages* » qui provoquent directement à des actes de terrorisme**, quelle que soit la forme que prendrait ce message ;

– les sites faisant l'apologie d'actes de terrorisme, lorsqu'ils comportent des « *images montrant la commission d'actes de terrorisme consistant en des atteintes volontaires à la vie* », formulation reprise du 1° de l'article 421-1 du code pénal précité. Dans cette seconde hypothèse, centrer le délit de consultation habituelle sur les seules *images* permet non seulement d'**objectiver plus facilement la constitution de l'infraction**, mais surtout de répondre aux enjeux contemporains de la propagande terroriste sur internet : comme l'a souligné le juge Marc Trévidic, aujourd'hui, « ***le vecteur de radicalisation change et l'image l'emporte sur l'écrit***. *Dans cette civilisation de l'image, les vidéos jihadistes ont plus de succès que les écrits des théoriciens du Jihad* » [(3)].

Toutefois, afin de tenir compte de l'existence de certains motifs légitimes de consultation de sites internet faisant l'apologie du terrorisme, le délit créé à l'article 2 de la présente proposition **ne serait pas applicable lorsque cette consultation résulte de l'exercice normal d'une profession ayant pour objet d'informer le public, intervient dans le cadre de recherches scientifiques ou est réalisée afin de servir de preuve en justice**. Les journalistes et les chercheurs ne seraient ainsi pas concernés.

Le nouveau délit serait, comme en matière de pédopornographie, **puni de deux ans d'emprisonnement et de 30 000 euros d'amende**.

À la différence des autres infractions de terrorisme, **la procédure pénale applicable serait adaptée, afin de la rapprocher du droit commun** et, ainsi, de respecter au mieux les droits et libertés constitutionnellement garantis.

L'**article 3** de la proposition de loi dispose en ce sens que :

– le délai de *prescription* de l'action publique serait de trois ans, et non de vingt ans comme les autres délits de terrorisme ;

– la *garde à vue* serait régie par les règles de droit commun, plutôt que par les normes spécifiques au terrorisme ;

– les *perquisitions* de nuit seraient interdites.

---

(1) Le champ d'application de l'article 2 est plus restreint que celui de l'article 1er, qui permet de bloquer l'accès à des sites internet faisant l'apologie du terrorisme.

(2) La distinction retenue s'inspire de la rédaction prévue au sixième alinéa de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse, précédemment évoqué.

(3) Terroristes. Les sept piliers de la déraison, ibid., *p. 81.*

En revanche, les *autres* règles de procédure spécifiques à la répression du terrorisme seraient applicables au nouveau délit de consultation habituelle de sites faisant l'apologie du terrorisme, en particulier la centralisation des affaires à Paris et les règles régissant la surveillance des personnes, les infiltrations, les interceptions de correspondances, les sonorisations et fixations d'images et la captation de données informatiques.

Naturellement, l'édiction de ce nouveau délit de consultation habituelle de sites faisant l'apologie du terrorisme ne saurait suffire à mettre fin, à elle seule, à la fabrique d'apprentis terroristes. Mais ce délit pourrait constituer une très utile « accroche », permettant de **repérer certains individus en voie de radicalisation**.

Les modalités actuelles de répression de la pédopornographie peuvent d'ailleurs, *mutatis mutandis*, offrir une comparaison pertinente : en pratique, la poursuite de prévenus sur le terrain de la seule *consultation* de sites pédopornographiques permet souvent de découvrir, dans un second temps de l'enquête, la *détention*, voire la *diffusion*, d'images ou de vidéos pornographiques mettant en scène des mineurs. En d'autres termes, la poursuite pour « simple » consultation est fréquemment une porte d'entrée conduisant à la répression d'autres infractions.

Le nouveau délit proposé à l'article 2 permettrait également de sanctionner ce qui pourrait s'apparenter à la commission d'**actes préparatoires objectivant un *projet* terroriste**. C'est, en cela, un début de réponse [(1)] au constat, dressé notamment par le juge Marc Trévidic, selon lequel notre droit pénal est « *inadapté pour empêcher le départ de Français ou neutraliser les velléités d'actes* ***individuels****, l'association de malfaiteurs n'étant caractérisée que s'il existe un minimum de contacts avec des tiers* » – ce qui rendrait nécessaire la création d'une nouvelle infraction qui « *pourrait viser la préparation d'un acte terroriste objectivée par plusieurs faits matériels, tels que* ***la consultation habituelle de sites internet de propagande****, l'acquisition de composants ou de produits explosifs, le repérage de cible, l'entraînement militaire et les mouvements financiers suspects* » [(2)].

Lors de son audition par votre rapporteur, M. Marc Trévidic s'est d'ailleurs montré explicitement favorable à l'édiction de ce nouveau délit de consultation habituelle de sites, comme instrument supplémentaire de lutte contre les individus isolés en voie de radicalisation.

Enfin, créer un délit de consultation habituelle de sites internet provoquant au terrorisme ou faisant son apologie fournirait également **un puissant moyen de protection des mineurs**. Cet enjeu est essentiel, au regard de la précocité grandissante des jeunes endoctrinés par l'intermédiaire des réseaux sociaux. Le juge Marc Trévidic souligne en ce sens qu'il est de plus en plus fréquent que des

---

(1) Un début seulement, la question excédant le champ de la seule problématique de la propagande sur internet.

(2) Marc Trévidic, Jean-Charles Brisard et Thibault de Montbrial, ibid.

mineurs soient impliqués dans des affaires de terrorisme, ce qui était très rare avant le début des années 2000 [(1)]. Or, si dans notre société, un jeune homme de quinze ans est un mineur (notamment au plan pénal), pour les djihadistes, un individu devient majeur au moment de la puberté, l'autorisant alors à combattre au nom de la guerre sainte.

Dès lors que la consultation habituelle de sites faisant l'apologie du terrorisme serait érigée en délit, **toute personne qui inciterait un mineur à se livrer à une telle consultation tomberait sous le coup de l'article 227-21 du code pénal, qui réprime la « corruption de mineur »** : « *le fait de provoquer directement un mineur à commettre un crime ou un délit est puni de cinq ans d'emprisonnement et de 150 000 euros d'amende* ». Le délit en question serait celui créé à l'article 2 de la présente proposition de loi.

D. L'ÉLARGISSEMENT DES MOYENS DES « CYBERPATROUILLEURS »

L'**article 4** de la présente proposition de loi vise à **élargir le champ des infractions pour lesquelles il est possible de recourir aux techniques spéciales d'investigation que sont les « cyberpatrouilles »**.

Les « cyberpatrouilleurs » sont des officiers ou agents de police judiciaire intervenant sur internet afin de constater la commission de certaines infractions par des moyens spécialement adaptés : participation sous un pseudonyme à des échanges électroniques ; mise en contact avec les personnes susceptibles de commettre ou d'avoir commis ces infractions ; extraction de données et d'éléments de preuve. Conformément au principe de loyauté de la preuve, ils ne sont cependant pas autorisés à inciter à la commission des infractions en question.

En matière de terrorisme, ces moyens spécifiques d'investigation ont été introduits dès 2011, **dans la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, dite « LOPPSI 2 » – qui témoignait ainsi de la volonté d'adapter notre arsenal juridique aux évolutions techniques et aux nouvelles formes de menaces**.

Ainsi, les « cyberpatrouilles » permettent aujourd'hui la répression des infractions de provocation directe aux actes de terrorisme ou d'apologie de tels actes (article 706-25-2 du code de procédure pénale, renvoyant au sixième alinéa de l'article 24 de la loi de 1881 précitée).

L'article 4 de la proposition de loi **étendrait cette technique d'investigation à la constatation du délit de consultation habituelle de certains sites faisant l'apologie du terrorisme**, créé à l'article 2.

Plusieurs fois mise en avant – jusqu'à présent sans succès – par le soussigné et par les autres députés de son groupe, **la nécessité de renforcer les**

(1) Terroristes. Les sept piliers de la déraison, ibid., *p. 82.*

possibilités de « cyberpatrouilles » est désormais reconnue par le ministre de l'Intérieur. Entendu le 30 avril 2014 par votre commission des Lois, M. Bernard Cazeneuve a ainsi convenu qu'il était « *crucial, pour pouvoir lancer des poursuites judiciaires, que nous pénétrions ces réseaux qui recrutent grâce aux forums, aux réseaux sociaux et autres multiples moyens de communication disponibles sur l'internet. Cette partie du dispositif exigera l'adoption de mesures législatives pour permettre l'intervention de nos enquêteurs sous pseudonyme* » [(1)]. L'article 4 de la proposition de loi s'inscrit dans ce cadre.

Au-delà, en raison de la vitesse à laquelle la menace terroriste évolue sur internet, votre rapporteur souligne que **la lutte contre le terrorisme supposera certainement d'aller plus loin, en créant un dispositif législatif autorisant les « cyberpatrouilles » à des fins de police administrative** – c'est-à-dire dans une optique préventive [(2)].

Concrètement, en s'inspirant du dispositif récemment adopté pour la géolocalisation administrative en temps réel et du régime applicable aux interceptions administratives de sécurité [(3)], **les cyberpatrouilles visant à prévenir les actes de terrorisme pourraient être soumises à l'autorisation du Premier ministre, mises en œuvre par les services spécialisés du ministère de l'Intérieur et faire l'objet d'un contrôle par l'autorité administrative indépendante qu'est la Commission nationale des interceptions de sécurité (CNCIS)** [(4)].

La durée de l'autorisation délivrée par le Premier pourrait être fixée à soixante jours (renouvelables), soit une durée intermédiaire entre celle en vigueur en matière de géolocalisation en temps réel – trente jours – et celle applicable aux interceptions de sécurité – quatre mois. Compte tenu de son caractère innovant et spécifique à la prévention du terrorisme, ce dispositif pourrait être créé, dans un premier temps, sous la forme d'une expérimentation, valable par exemple pour une période de deux ans.

Naturellement, la mise en place de ces nouveaux outils s'ajouterait, sans s'y substituer, aux moyens et prérogatives dont disposent d'ores et déjà les

---

(1) Compte rendu de la commission des Lois n° 52 du 30 avril 2014.

(2) Voir en ce sens l'amendement CL16 portant article additionnel après l'article 4 présenté par votre rapporteur, rejeté par votre commission des Lois.

(3) Respectivement : article 20 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale ; articles L. 241-1 et suivants du code de la sécurité intérieure.

(4) En application de l'article L. 243-2 du code de la sécurité intérieure, celle-ci est composée de trois membres : un président désigné par le chef de l'État, sur une liste de quatre noms établie conjointement par le vice-président du Conseil d'État et le premier président de la Cour de cassation ; un député désigné pour la durée de la législature par le président de l'Assemblée nationale (actuellement : M. Jean-Jacques Urvoas, président de votre commission des Lois) ; un sénateur désigné après chaque renouvellement partiel du Sénat par le président du Sénat (actuellement : M. Jean-Jacques Hyest).

services de renseignement – par exemple la faculté de recourir à une identité d'emprunt pour mener à bien certaines missions [(1)].

Au total, **adopter la présente proposition de loi placerait la France à l'avant-garde du combat contre le cyberdjihadisme, à charge pour le chef de l'État et le Gouvernement de porter ce débat au sein des instances européennes et, au-delà, au plan international, notamment transatlantique** – la coopération entre les États étant absolument indispensable en la matière. **C'est le devoir de la France que d'être en pointe sur ce sujet majeur**, compte tenu du nombre de nos ressortissants concernés par un départ en Syrie.

(1) Issu de la « LOPPSI 2 » de 2011, l'article L. 2371-1 du code de la défense dispose ainsi : « Pour l'exercice d'une mission intéressant la défense et la sécurité nationale, les agents des services spécialisés de renseignement peuvent, sous l'autorité de l'agent chargé de superviser ou de coordonner la mission, faire usage d'une identité d'emprunt ou d'une fausse qualité.

« Dans ce cas, ne sont pas pénalement responsables de cet usage les agents mentionnés au premier alinéa, non plus que de leurs actes les personnes requises à seule fin d'établir ou de permettre l'usage de l'identité d'emprunt ou de la fausse qualité (…). »

DISCUSSION GÉNÉRALE

Lors de sa séance du mercredi 4 juin 2014, la Commission examine, sur le rapport de M. Guillaume Larrivé, la proposition de loi renforçant la lutte contre l'apologie du terrorisme sur internet, présentée par MM. Guillaume Larrivé, Éric Ciotti, Philippe Goujon et Olivier Marleix (n° 1907).

M. le président Jean-Jacques Urvoas. La première proposition de loi que notre Commission examinera ce matin a été inscrite par le groupe UMP à l'ordre du jour de l'Assemblée nationale la semaine prochaine.

Monsieur le rapporteur, je vous prie par avance de m'excuser si j'étais empêché d'assister à ce débat en séance publique. Je dois en effet conduire une délégation de la Délégation parlementaire au renseignement à Washington, où nous rencontrerons pour la première fois nos homologues du Sénat et de la Chambre des représentants, qui contrôlent depuis quelques années déjà les services de renseignement américains. Nous avons pensé qu'il pouvait être utile de confronter notre compétence nouvelle et leur expérience, comme nous l'avons fait avec l'*Intelligence Service Committee* à la Chambre des communes britannique.

M. Guillaume Larrivé, rapporteur. Les menaces terroristes qui pèsent sur notre pays sont une réalité renouvelée que chacun, hélas, a aujourd'hui à l'esprit. Elles appellent une réponse très déterminée, opérationnelle autant que juridique, de la part de l'ensemble des partis de gouvernement.

Nous savons que le Gouvernement prépare un projet de loi renforçant notre arsenal antiterroriste et qu'il participe, au plan européen, à un nécessaire effort de coordination en ce sens. Le groupe UMP entend prendre toute sa part à la préparation de ces mesures d'intérêt général. C'est le sens de la proposition de loi que j'ai l'honneur de vous présenter avec MM. Éric Ciotti, Philippe Goujon et Olivier Marleix.

Nous ne prétendons pas embrasser l'ensemble des questions posées par la lutte contre le terrorisme. Nous avons eu et nous aurons d'autres débats à cette fin. La proposition de loi est centrée sur un objet précis : la lutte contre la diffusion du terrorisme au moyen d'internet.

Le texte que nous vous proposons et les amendements qui l'accompagnent sont nourris par de nombreuses auditions – ont ainsi été entendus les responsables opérationnels de la lutte antiterroriste et des services de renseignement, l'Office de lutte contre la cybercriminalité, le juge antiterroriste Marc Trévidic, l'association des victimes du terrorisme, l'imam Chalghoumi, président de la Conférence des imams de France, la direction du Conseil représentatif des institutions juives de France (CRIF) et des acteurs et opérateurs d'internet.

Ces auditions ont renforcé notre conviction qu'internet est aujourd'hui un vecteur majeur, sans doute le premier, de la propagande djihadiste et, par conséquent, le principal moyen d'endoctrinement d'individus susceptibles de se livrer, de manière isolée ou collective, à un attentat terroriste.

À titre d'illustration, je vous invite, mes chers collègues, à vous reporter au dernier numéro, malheureusement très facile à trouver sur internet, de la revue en ligne *Inspire*, diffusée par la nébuleuse d'Al-Qaïda dans la péninsule arabique (AQPA), qui vise à diffuser le djihad au sein du monde occidental. Vous y trouverez notamment un mode d'emploi très précis pour la fabrication de bombes et des conseils pratiques, eux aussi très précis, pour commettre des attentats en France. Vous pourrez également constater, en un ou deux clics, qu'il est très aisé d'accéder à des vidéos présentant, pour les glorifier, des scènes de décapitation par des djihadistes, vues par des dizaines de milliers d'internautes.

Il y a aujourd'hui urgence à réagir. Nos ennemis terroristes ont investi un champ de bataille sur lequel les démocraties ne sont pas encore suffisamment entrées et pour lequel elles sont encore désarmées.

Il existe, bien sûr, des moyens de veille de l'internet et je ne sous-estime pas le travail effectué en ce sens par les agents affectés au sein de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Le nombre de signalements de sites de propagande terroriste que reçoit l'Office ne cesse d'augmenter : alors que 13 signalements de ce type avaient été enregistrés en 2011, ce nombre est passé à 120 en 2012, pour atteindre 360 en 2013, soit près d'un signalement par jour. En 2013, les principaux sites concernés par ces signalements ont été les réseaux sociaux, en particulier Facebook et Twitter, qui représentaient 54 % du total, puis des blogs, pour 14 %, des sites internet thématiques, pour 13 %, la plateforme YouTube, pour 6 %, et de forums, pour 6 %. Chaque signalement fait l'objet d'un traitement individuel, qui peut aboutir à la saisine de l'autorité judiciaire.

Notre conviction est qu'il faut aller bien au-delà de la simple veille.

Je propose à cette fin quatre mesures, directement inspirées du projet de loi qui avait été présenté dès avril 2012, sous l'impulsion du président Nicolas Sarkozy, par le gouvernement de l'époque, et des amendements que j'avais présentés avec Éric Ciotti, Nathalie Kosciusko-Morizet et Philippe Goujon en novembre 2012, lors de l'examen du projet de loi relatif à la sécurité et à la lutte contre le terrorisme. Ces amendements, retravaillés au fil des auditions, constituent le socle de cette proposition.

Première mesure : nous voulons renforcer les obligations de signalement qui pèsent sur les fournisseurs d'accès et les hébergeurs de sites.

Depuis la loi du 21 juin 2004, ces opérateurs ont la double obligation de mettre en œuvre un dispositif permettant à toute personne de porter à leur connaissance des contenus illicites relatifs à l'apologie de crimes contre

l'humanité, à la provocation à la haine, à la diffusion d'images pédopornographiques et à la diffusion de message portant atteinte à la dignité humaine, et d'informer les autorités publiques compétentes de ces activités illicites. Il s'agit donc d'un double mécanisme de signalement, de l'internaute à l'opérateur et de l'opérateur à l'autorité publique. En pratique, les signalements de contenus illicites sont centralisés auprès de l'OCLCTIC, qui gère une plateforme en ligne de signalement dénommée « PHAROS ».

Nous proposons que ce dispositif de vigilance soit explicitement étendu aux contenus faisant l'apologie du terrorisme, ce qui n'est aujourd'hui pas le cas en droit. Il faut que, demain, les fournisseurs d'accès à internet et les hébergeurs de sites aient l'obligation, de leur propre initiative et à peine de sanction, de signaler aux autorités les sites faisant l'apologie du terrorisme. Cette première mesure est le *minimum minimorum* que l'on puisse exiger des opérateurs de l'internet, sans doute trop enclins aujourd'hui à considérer que leur autorégulation est suffisante, ce qui n'est manifestement pas le cas.

Deuxième mesure : nous voulons donner la faculté aux services du ministère de l'Intérieur, d'obtenir le blocage de l'accès aux sites de propagande terroriste.

De quels sites parlons-nous ? La frontière est parfois ténue, il est vrai, entre les contenus publics et les contenus relevant de la correspondance privée. Nous voulons un dispositif qui s'applique aussi largement que possible aux contenus à caractère public, qu'il s'agisse de sites internet classiques, de blogs, de forums de discussion, de plateformes vidéo ou de pages de réseaux sociaux comme Facebook ou Twitter.

La proposition de loi et les amendements qui l'accompagnent prévoient cette possibilité de blocage pour tous les contenus faisant l'apologie du terrorisme ou provoquant aux actes de terrorisme, quelle que soit la forme du message : il peut, bien sûr, s'agir de vidéos, mais aussi d'images fixes, de sons ou d'écrits. La proposition de loi, telle qu'amendée par votre rapporteur, couvre bien tout ce champ.

Qu'appelle-t-on « bloquer » un site ? Il ne s'agit pas, par ce moyen, de chercher à obtenir la fermeture ou le retrait du contenu, ce qui est déjà théoriquement possible pour un contenu illicite, mais très difficile dans la pratique, la plupart de ces sites étant hébergés à l'étranger. Le blocage de l'accès est une mesure de police administrative, prise pour la sauvegarde de l'ordre public et ayant un caractère aussi opérationnel que possible : le site reste actif, mais les internautes français n'y ont plus accès. Quand il cherche à se connecter, l'utilisateur est renvoyé à une page internet lui indiquant que le site qu'il veut consulter n'est pas accessible, car tombant sous le coup de la loi. Concrètement, ce sont les fournisseurs d'accès à internet – par exemple Orange, Free, SFR ou Bouygues – qui auraient le devoir de bloquer l'accès à une série de sites définie

par le ministère de l'Intérieur sur une « liste noire » ciblée et actualisée dans la mesure du possible.

Il s'agit donc de donner aux services chargés de lutter contre le terrorisme un outil supplémentaire, souple et réactif, auquel ils pourraient recourir de manière discrétionnaire. Dans certains cas, ils pourront avoir intérêt à laisser perdurer l'accès à des sites internet, afin de pouvoir recueillir des renseignements sur ceux qui les fréquentent et sur les projets qu'ils préparent, mais dans d'autres cas, il faudra peut-être « couper le signal », afin d'éviter que la haine ne se propage sur les réseaux.

Ce dispositif, nous en sommes convaincus, va dans le sens des déclarations faites par le ministre de l'Intérieur lors de son audition par notre Commission, le 30 avril dernier : « nous agirons (...) auprès des opérateurs pour qu'ils "coupent" les discours, les vidéos et les images servant à l'endoctrinement ».

J'ajoute que le dispositif proposé s'inspire de celui, créé par la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, dite « LOPPSI 2 », applicable aux sites pornographiques diffusant des images de mineurs – dispositif explicitement examiné et validé par le Conseil constitutionnel.

On nous objectera sans doute que ce dispositif n'est toujours pas en vigueur, faute de publication par le Gouvernement d'un décret d'application. Il ressort cependant des auditions que j'ai menées qu'il n'y a là aucune impossibilité technique ou juridique, mais seulement une contrainte budgétaire, qui donne lieu à un débat entre le ministère de l'Intérieur et le ministère du Budget, la loi de 2011 prévoyant la compensation financière aux fournisseurs d'accès des surcoûts liés au blocage des sites pédopornographiques.

Au bout du compte, il n'y a aucun obstacle dirimant, ni au plan juridique, ni au plan opérationnel, pour définir et mettre en œuvre un tel dispositif de blocage des sites à caractère terroriste. Chacun doit prendre ses responsabilités. La nôtre, en notre qualité de législateur, est de nous engager dans ce dispositif.

Troisième mesure : la proposition de loi crée un nouveau délit réprimant la consultation habituelle de sites internet incitant au terrorisme. Là encore, nous nous inspirons du droit applicable en matière de lutte contre les images pornographiques de mineurs. Depuis 2007, l'article 227-23 du code pénal punit de deux ans d'emprisonnement et de 30 000 euros d'amende « le fait de consulter habituellement » un site internet diffusant des images pédopornographiques.

Les sites visés par la nouvelle incrimination seraient très précisément définis, afin de ne pas porter une atteinte disproportionnée à la liberté de communication et de ne sanctionner que la consultation des sites dont l'illégalité est manifeste. Concrètement, il s'agirait par exemple de sites montrant des décapitations ou des exécutions commises à des fins terroristes.

Naturellement, certains motifs légitimes de consultation seraient préservés, lorsque la consultation des sites en cause est justifiée par l'exercice normal d'une profession ayant pour objet d'informer le public, lorsqu'elle intervient dans le cadre de recherches scientifiques ou lorsqu'elle est réalisée afin de servir de preuve en justice.

Ce nouveau délit aurait deux avantages. D'une part, il permettrait de repérer et de sanctionner les individus en voie de radicalisation et de basculement dans la violence terroriste. Cela serait d'autant plus utile face à des individus qui, parce qu'ils sont isolés, ne peuvent pas entrer à, ce stade, dans le champ du délit d'association de malfaiteurs en lien avec une entreprise terroriste. Je précise que, lors de son audition, hier matin, le juge antiterroriste Marc Trévidic a explicitement indiqué qu'il était favorable à l'édiction de ce nouveau délit de consultation habituelle d'un site, comme instrument de lutte contre les « loups solitaires ».

D'autre part, ce délit de consultation habituelle permettrait de mieux protéger les mineurs, notamment ceux de 13 à 16 ans, qui sont les plus vulnérables aux stratégies d'endoctrinement – pour ne pas dire : de « lavage de cerveau » – que l'on peut trouver sur internet. Un individu qui inciterait un mineur à se livrer à une telle consultation pourrait ainsi être poursuivi pour « corruption de mineur », sur le fondement de l'article 227-21 du code pénal. Quant aux mineurs eux-mêmes, une peine alternative pourrait leur être réservée, telle qu'un stage de sensibilisation et de prévention adapté, comme le proposent notamment les associations qui participent, à l'échelle européenne, au réseau Radicalisation Awareness Network (RAN). Je vous proposerai tout à l'heure un amendement en ce sens, qui relève de l'idée que, face aux « prêcheurs de haine », il faut développer à l'intention des adolescents un contre-discours susceptible de les éloigner de la propagande radicale dont ils sont l'objet.

Quatrième et dernière mesure : la proposition de loi vise à renforcer les possibilités de « cyberpatrouilles » ou de « cyberinfiltrations » pour lutter contre le terrorisme.

Les « cyberpatrouilleurs » sont des policiers spécialement habilités, qui peuvent intervenir sur internet ou sur des réseaux sociaux pour y constater la commission de certaines infractions. Dans ce cadre, ils peuvent participer à des discussions sous un pseudonyme, entrer en relations avec des personnes et recueillir des données et des éléments de preuve, la seule limite étant de ne pas inciter directement à la commission des infractions en cause.

En matière de terrorisme, ces moyens d'investigation ont été introduits dès 2011 dans la LOPPSI 2. Il s'agissait d'une première adaptation de notre arsenal juridique aux évolutions techniques et aux nouvelles formes de menaces. Ces cyberpatrouilles permettent aujourd'hui, sous un régime de police judiciaire – et sous ce régime seulement –, de constater et de réprimer les infractions de provocation directe au terrorisme ou d'apologie du terrorisme.

La proposition de loi étend cette possibilité à la répression du nouveau délit de consultation habituelle des sites internet faisant l'apologie du terrorisme. Les cyberpatrouilleurs pourront ainsi repérer plus facilement les incitations aux idées extrémistes, les tentatives de recrutement terroriste et la préparation d'attentats.

Sans doute faudrait-il aller encore plus loin, en créant un dispositif législatif autorisant les cyberpatrouilles à des fins de police administrative, c'est-à-dire dans une optique préventive. Je vous présenterai tout à l'heure un amendement en ce sens, créant un nouveau régime juridique pour consolider des pratiques qui se situent actuellement dans un cadre juridique incertain.

Pour conclure, mes chers collègues, la lutte antiterroriste doit être un sujet qui nous rassemble au nom de l'intérêt général. Le groupe UMP n'a pas failli à cette nécessaire solidarité face à la menace terroriste et a voté, en novembre 2012, la loi antiterroriste présentée par le Gouvernement.

Nous invitons chacun à faire de même aujourd'hui, en adoptant cette proposition de loi renforçant la lutte contre l'apologie du terrorisme sur internet.

Ce serait placer la France à l'avant-garde du combat contre le cyber-djihadisme, à charge pour le pouvoir exécutif de porter activement ce combat au sein des instances européennes et, au-delà, à l'échelle internationale, notamment transatlantique. C'est notre devoir que d'être en pointe sur ce sujet majeur, pour lequel nos démocraties sont aujourd'hui, hélas, encore trop désarmées.

M. le président Jean-Jacques Urvoas. Je suis heureux d'accueillir monsieur le ministre de l'Intérieur qui vient de nous rejoindre. Monsieur le ministre, vous êtes le bienvenu aux réunions de la commission des Lois.

La proposition de loi qui nous est soumise part d'un constat que nous avons déjà souvent évoqué ici : internet prend à l'évidence une part déterminante dans la radicalisation, le recrutement et la propagande qui visent à nuire aux intérêts fondamentaux de la nation. Il appartient donc au législateur de trouver des outils pour combattre ces menaces et nous avons à cet égard une perspective commune et une ambition partagée. L'essentiel de notre débat sera donc probablement technique : les outils proposés sont-ils adaptés ?

À titre personnel, je ne suis pas insensible, monsieur le rapporteur, à votre première proposition, consistant à étendre les obligations de surveillance sur les sites faisant l'apologie du terrorisme. D'autres dispositions proposées nous sont déjà bien connues. En effet, M. Michel Mercier, garde des Sceaux, avait présenté un projet de loi après l'affaire Merah et vous aviez déjà déposé en juillet 2012 une proposition de loi sur ce sujet. Par ailleurs, M. Manuel Valls avait évoqué des interrogations quant à des risques d'inconstitutionnalité lors de l'examen du projet de loi relatif à la sécurité et à la lutte contre le terrorisme, dont Mme Marie-Françoise Bechtel était rapporteure en novembre 2012.

Je crois donc pouvoir vous dire que la Commission examinera votre texte avec un *a priori* favorable, mais que nous avons encore aujourd'hui des interrogations techniques expliquant que certains points ne recueilleront probablement pas l'unanimité, et pourraient même se heurter à une hostilité majoritaire. Il ne s'agit cependant pas là d'un refus de prendre en compte les questions que vous soulevez, et cela d'autant moins que le Gouvernement proposera prochainement un projet de loi qui fixe le même objectif et la même ambition, dont je ne doute pas qu'ils soient ici unanimement partagés.

M. Bernard Cazeneuve, ministre de l'Intérieur. Je vous remercie, monsieur le Président, mesdames, messieurs les députés de m'accorder l'hospitalité pour l'examen en commission de cette proposition de loi.

J'ai souhaité participer aux travaux de votre Commission à l'occasion d'une initiative émanant de l'opposition, car j'ai la conviction que, sur les questions relatives à la lutte contre le terrorisme et le djihadisme, nous devons autant que faire se peut rechercher des solutions efficaces ensemble et laisser de côté les clivages classiques de la politique, car ces sujets sensibles doivent faire l'objet d'un traitement dénué de tout esprit polémique et mobiliser toutes les initiatives afin que les meilleures solutions soient arrêtées au profit de la sécurité du pays.

Le développement insidieux de la pensée radicale djihadiste est un phénomène très inquiétant, que nous constatons sur l'ensemble du territoire national comme dans un très grand nombre de pays de l'Union européenne – voire dans tous –, avec un processus très bien pensé d'endoctrinement et de recrutement de jeunes gens vivant parmi nous et ressortissants de nos propres pays, où la plupart sont nés et ont grandi. Il n'y a rien de plus insupportable pour un élu de la République que de constater que, sur son territoire, les prêcheurs de haine aient pu recruter des jeunes qui n'étaient pas tous prédisposés à basculer.

En me rendant parmi vous ce matin, je veux dire mon désir d'être à vos côtés afin que nous puissions tout mettre en œuvre pour faire échec aux stratégies d'embrigadement que mènent ces groupes radicaux et terroristes.

La proposition de loi présentée par M. Guillaume Larrivé est une initiative qui permet de poser des questions intéressantes, que nous nous posons tous et auxquelles nous nous efforçons d'apporter des réponses pertinentes. Je sais que, dans le cadre de vos travaux préparatoires, vous avez notamment auditionné le directeur général de la sécurité intérieure et le directeur des libertés publiques et des affaires juridiques du ministère de l'Intérieur, qui restent à votre entière disposition pour tenter de trouver avec vous des solutions pour lutter le plus efficacement contre le terrorisme.

Monsieur Larrivé, je partage les préoccupations qui ont inspiré vos travaux et votre proposition de loi. Les sites internet qui font l'apologie du terrorisme constituent plus qu'une menace : nous savons désormais qu'ils sont le vecteur

essentiel de l'endoctrinement vers la radicalisation violente, au nom d'objectifs parfois prétendument humanitaires ou d'une pensée religieuse dévoyée. Ils conduisent en particulier, au phénomène dit des « loups solitaires », qui se développe dangereusement et concerne des personnes qui, par nature, ne sont pas facilement détectables. Au demeurant, le contenu de cette notion de « loup solitaire » est incertain et il faut l'utiliser avec prudence. De fait, s'il est possible que ces personnes basculent seules dans la violence à la suite d'une relation, exclusive de toute autre, avec la violence sur internet, et qu'ils agissent de leur propre initiative, ils peuvent aussi, tout en agissant seuls, bénéficier de complicités ou être intégrés dans des groupes. Ainsi, comme le montrent les cas les plus récents, il faut généralement attendre que les enquêtes parviennent à leur terme pour savoir quels sont exactement les profils, les complicités, les cercles rencontrés et les moyens collectifs mobilisés. Je comprends toutefois la nécessité de traiter le basculement d'individus dans le djihadisme par la consultation d'internet.

Vous proposez le principe d'une incrimination de la consultation habituelle de sites aux contenus terroristes. Cette préoccupation, comme l'a reconnu le Président de votre Commission, est parfaitement louable et l'on devine sans peine les motivations qui la sous-tendent. Cependant, le Conseil d'État, depuis l'examen du projet de loi antiterroriste de 2012, considère cette incrimination comme constituant ou pouvant constituer une violation disproportionnée de la liberté d'opinion et de communication garantie par la Constitution. Je ne crois pas qu'il faille pour autant éluder la question de la consultation des sites internet à caractère djihadistes, afin d'éviter les phénomènes de radicalisation, et je partage comme vous la préoccupation exprimée par le juge Trévidic.

C'est la raison pour laquelle j'invite la Commission à ne pas voter cette disposition qui ne pourra pas prospérer en l'état, ni les articles qui en découlent. En revanche, je vous propose de travailler dans la perspective du projet de loi « sécurité » que je présenterai au conseil des ministres à la fin du mois de juin et qui sera débattu au Parlement le plus rapidement possible, texte qui inclura des dispositions contre les dérives djihadistes et sera soumis à votre examen rapide. Nous pourrons ainsi examiner à nouveau cette question essentielle après avoir fait le tour de ses aspects juridiques, afin de nous assurer que nous ne prenons aucun risque de voir retoquer ce dispositif.

La proposition de loi prévoit également, dans son article l^{er}, deux éléments distincts. Il s'agit tout d'abord d'appliquer aux sites faisant l'apologie du terrorisme le même régime qu'à ceux qui font l'apologie des crimes contre l'humanité, incitent à la haine raciale ou diffusent des contenus pédopornographiques. J'y suis absolument favorable et, plus encore, je suis favorable à étendre cette disposition à la provocation, comme vous le proposez, monsieur le rapporteur, dans un amendement.

Doit-on aussi proposer le blocage de ces sites ? Les instances européennes nous ont encouragés à le faire pour ce qui relève des sites pédopornographiques, mais nous rencontrons des difficultés objectives de mise en œuvre effective de ces dispositions. En effet, le Conseil constitutionnel, dans une de ses décisions, considère qu'un tel blocage, qui relève d'une logique d'ordre public, doit faire l'objet d'une compensation financière de l'État aux fournisseurs, ce qui pourrait représenter une mobilisation significative de fonds publics. Or, à quel titre dépenserait-on des fonds publics en compensation d'éléments illégaux diffusés par les fournisseurs d'accès ? Nous négocions donc durement avec ces derniers pour obtenir qu'ils se conforment rigoureusement au droit, sans aucune contrepartie.

M. Philippe Goujon. Monsieur le ministre, nous partageons le diagnostic et les objectifs. Nul ici, en effet, n'ignore les difficultés juridiques et matérielles liées à l'application d'un tel texte au regard de la nécessaire protection des libertés publiques et individuelles et de la complexité d'une appréhension d'ensemble de la planète internet. Cependant, compte tenu de l'extrême urgence qu'il y a à agir, renvoyer ce texte, dont vous avez vous-même reconnu l'importance, à un texte ultérieur dont nous serons peut-être saisis dans quelques mois ne peut nous satisfaire. Faut-il rappeler que près de 300 de nos compatriotes sont partis faire le djihad en Syrie – chiffre en hausse de 75 % sur les six derniers mois ? Qu'en sera-t-il dans six mois si ce texte n'est pas appliqué ? La question est d'autant plus urgente que la plupart des personnes qui se rendent sur ces théâtres d'opérations en sont convaincues par le biais d'internet et que, comme l'a rappelé le rapporteur, l'un des magazines djihadistes les plus consultés sur internet, qui indique comment fabriquer de bombes artisanales, cible particulièrement notre pays.

Une étude du Centre de prévention des dérives sectaires liées à l'islam a révélé la présence importante de femmes – 40 % – dans ce contingent d'apprentis djihadistes, à 70 % originaires de famille athées, membres de la classe moyenne dans leur immense majorité – 83 % –, voire de familles aisées pour 20 % d'entre elles. Ce qui est en cause est donc moins la misère sociale que la perte de repères de jeunes gens « normaux », aiguillonnés par des sites internet qui prennent à distance le contrôle de leur vie, selon des procédés qui sont ceux des dérives sectaires et dont la pénétration est facilitée par le vecteur internet.

Notre groupe a voté la loi de lutte contre le terrorisme du 21 décembre 2012, qui reprenait d'ailleurs en partie des dispositions portées par la précédente majorité à la suite de l'affaire Merah et répondait à la nécessité de pérenniser le cadre juridique établi par la loi antiterroriste de 2006. Cette volonté commune de garantir la sécurité de nos compatriotes et de notre pays nous rassemble bien évidemment au-delà de nos appartenances politiques. C'est dans cet esprit que la proposition de loi que nous examinons vise à fournir des outils juridiques permettant d'agir en amont pour mettre hors circuit ces terroristes potentiels.

La possibilité de bloquer les sites djihadistes, proposée par l'article 1er, complète le panel d'outils de police administrative mis à la disposition des forces de sécurité, sans pour autant empêcher la pratique du cybersuivi et du harponnage

des suspects actuellement utilisée par les services. Notre rapporteur propose à juste titre d'élargir encore le champ du dispositif de blocage, notamment pour y inclure, outre les images, les contenus audio et textuels que l'on trouve aussi très fréquemment sur ces sites.

L'article 2 s'inspire d'un amendement, rejeté par le Gouvernement, que MM. Éric Ciotti et Guillaume Larrivé, Mme Nathalie Kosciusko-Morizet et moi-même avions porté lors des débats sur la loi de lutte contre le terrorisme, en vue de créer ce délit de consultation habituelle des sites faisant l'apologie du terrorisme. En intégrant ce délit dans notre droit, nous mettrons en outre notre législation en conformité avec le mémorandum de Rabat, signé par les membres du Forum mondial contre le terrorisme, auquel la France appartient et qui préconise la criminalisation des actes préparatoires. Il permettra, sous la compétence de la juridiction parisienne et, bien sûr, selon le code pénal, d'arrêter les suspects et de les placer en garde à vue afin de recueillir des informations permettant de déterminer leur degré d'endoctrinement et de dangerosité. Ce délit constituera également une base très utile pour inculper de corruption de mineur un majeur ayant poussé un mineur à consulter ces sites, et de lutter ainsi contre le départ des mineurs. Il jouera également un rôle dissuasif auprès des primo-consultants de ces sites. Un amendement du rapporteur sera présenté à ce propos, afin de compléter la réponse pénale destinée aux mineurs, prévoyant notamment un stage de désendoctrinement, solution qui existe déjà pour les délits raciaux.

Enfin, les cyberpatrouilleurs prévus par la LOPPSI 2 seront renforcés par cette proposition de loi qui permettra, en matière de police judiciaire, d'effectuer surveillance, infiltration, sonorisation et captation de données informatiques lors de l'enquête de flagrance ou de l'enquête préliminaire. Là aussi, le texte sera amélioré par un amendement du rapporteur qui clarifiera le cadre légal d'exercice des cyberpatrouilles en matière de police administrative.

Ce texte a donc été très travaillé et présenté à plusieurs reprises. Il a été réfléchi et discuté avec les différents directeurs de vos services, monsieur le ministre, et certains magistrats spécialisés.

Nous avons bien entendu vos arguments, qui ne sont nullement hostiles à ce texte, mais nous pensons que, dans la situation présente, nous ne pouvons pas prendre le risque de perdre encore plusieurs mois dans la lutte contre le terrorisme en attendant un texte gouvernemental. Cette proposition de loi répond à un aspect du problème très urgent et les mesures qu'elle contient peuvent être mises en œuvre très rapidement pour lutter contre l'apologie du terrorisme et la provocation à celui-ci sur internet. C'est là une priorité pour éviter de nouveaux endoctrinements et autant de futures menaces pour notre sécurité nationale. L'augmentation du nombre de djihadistes a été, je le répète, de 75 % au cours des six derniers mois : de combien sera-t-elle dans les mois qui s'écouleront dans l'attente de votre texte ?

Nous avons voté la loi antiterroriste de décembre 2012 présentée par le Gouvernement et nous espérons que celui-ci et la majorité feront preuve du même esprit constructif à l'égard de cette proposition de loi.

Mme Marie-Françoise Bechtel. Nous nous inscrivons ici dans un esprit de coopération, à la recherche de mesures d'intérêt général que nous avons tous intérêt à adopter de la meilleure manière possible, lorsqu'elles seront prêtes à être opérationnelles juridiquement – et donc factuellement.

La proposition de loi que nous examinons s'inscrit dans une séquence qui commence avec la LOPPSI 2, se poursuit avec la loi antiterroriste (LAT) de décembre 2012, dont j'ai eu l'honneur d'être rapporteure et qui faisait suite partiellement au projet de loi Mercier. Cette séquence est également marquée par une double annonce ministérielle : lorsque nous avons examiné la LAT, le ministre de l'Intérieur, qui était alors M. Manuel Valls, avait annoncé qu'il faudrait améliorer certaines dispositions, relatives notamment au cyberpatrouillage, laissant la porte ouverte à une ou deux autres possibilités, selon l'évolution des choses. Hélas, cette évolution a conduit M. Cazeneuve à exprimer devant cette même Commission – et c'est le dernier acte de cette séquence –, qu'il était maintenant nécessaire de renforcer le dispositif antiterroriste – c'était avant l'affaire de Bruxelles, mais la situation était assez préoccupante et vous l'avez décrite avec beaucoup de précision, monsieur le ministre, voilà deux ou trois semaines. Il y a donc lieu de préciser certaines dispositions législatives et, sans doute, d'en introduire d'autres : c'est le travail auquel se livre également le Gouvernement. Il faut donc comprendre la proposition de loi que nous examinons comme un élément de réflexion et de travail auquel participe précisément notre discussion de ce matin.

À propos du texte, je soulignerai trois points majeurs, qui ont en commun la question fondamentale de savoir comment mieux appréhender le passage de la pensée à l'action djihadiste.

Tout d'abord, comment lutter contre l'apologie si les hébergeurs et fournisseurs d'accès laissent passer de nombreuses vidéos atroces qui posent le double problème de l'endoctrinement du majeur et de l'impression faite sur le mineur ? Le texte propose, et le ministre s'y est déclaré favorable, d'étendre la responsabilité des fournisseurs d'accès et hébergeurs, outre l'apologie de crimes contre l'humanité et la pédopornographie, qui figurent déjà au code pénal, à l'endoctrinement djihadiste par des vidéos violentes.

La deuxième question, qui nous a déjà divisés et risque de diviser encore, est celle de la « consultation habituelle » de sites. C'est là un point dont nous avons longuement débattu en commission durant la procédure d'adoption de la LAT. Nous y reviendrons sans doute dès aujourd'hui, et peut-être à la faveur d'amendements qui pourraient être déposés lors de l'examen du projet de loi du Gouvernement. Tel qu'il est aujourd'hui rédigé, en effet, le texte ne paraît pas satisfaire aux exigences de constitutionnalité et de proportionnalité. Il ne suffit pas

de dire qu'on peut avoir un motif légitime de consulter ces sites pour échapper au risque constitutionnel. De fait, le motif légitime peut avoir un champ très large – il peut même s'agir, ne craignons pas de le dire, de la simple curiosité intellectuelle. Or, nous n'avons pas à porter atteinte à des libertés en leur imposant un carcan sans souplesse. Cette partie de la proposition de loi devrait donc être difficile à reprendre, même ultérieurement.

Enfin, il faut saluer l'effort visant à renforcer le dispositif judiciaire et, surtout, administratif offert au cyberpatrouillage, sans aller jusqu'à la provocation à l'acte terroriste, défaut parfois dénoncé par la presse outre-Atlantique – peut-être aurez-vous, monsieur le président, l'occasion de faire prochainement le bilan de ces actions avec vos interlocuteurs américains. Il y a en tout cas matière à renforcer le cyberpatrouillage, comme nous en convenions du reste en votant la LAT en novembre 2012.

Il ne me semble pas choquant d'attendre quelques mois que nous soyons saisis d'une loi qui soit à la fois susceptible d'intégrer certaines des réflexions portées par la présente proposition de loi et plus achevée du point de vue de la sécurité juridique – c'est au contraire le meilleur moyen d'éviter le risque de retarder une action désormais de plus en plus urgente.

M. Sergio Coronado. Vous rappelez à juste titre, monsieur le Président, les constats communs que nous dressons face à la radicalisation de certains individus et à leur passage à l'acte. Nous souhaitons tous combattre le terrorisme, dans le respect des libertés et de l'État de droit, et je vous remercie de l'avoir rappelé dès le début de notre débat.

La présence ce matin du ministre de l'Intérieur dans notre Commission exprime en outre toute sa mobilisation dans cette lutte contre le terrorisme, sur laquelle l'actualité nous invite précisément à trouver sereinement un consensus.

Nous disposons déjà d'un arsenal antiterroriste complet et il ne faudrait pas laisser croire aux Français que nous en sommes encore à tâtonner au début de notre réflexion sur ce sujet. Cet arsenal s'est construit au fil des ans : tous les deux ou trois ans, en effet, nous discutons de dispositifs antiterroristes – la dernière fois était en 2012 et nous apprenons qu'un nouveau texte sera bientôt présenté en conseil des ministres.

Les écologistes préfèrent discuter sur le texte gouvernemental plutôt que sur la proposition de loi de M. Larrivé, qui comporte des dispositions problématiques. Il est, à cet égard, intéressant de s'interroger sur la doctrine gouvernementale. La proposition de loi introduit en effet des dispositions qui avaient déjà été rejetées par la majorité dans le débat de 2012, non par dogmatisme, mais parce que nous considérions qu'elles n'étaient pas techniquement réalisables et posaient plusieurs problèmes de respect de l'État de droit et des libertés fondamentales. Je rappelle également que la loi sur la consommation du 17 mars 2014 a abrogé l'article 18 de la loi du 21 juin 2004 sur

la confiance dans l'économie numérique, qui permettait potentiellement à l'autorité administrative de bloquer des sites internet au nom de divers motifs.

Comme l'a relevé Mme Bechtel, le texte ne règle pas la question de la proportionnalité, ni celle du blocage administratif, que nous avons déjà abordée à de nombreuses occasions.

Monsieur le ministre, l'article 6 de la loi du 21 juin 2004, relatif au blocage administratif des sites pédopornographiques, avait fait consensus, mais les spécialistes des aspects techniques de l'internet avaient souligné la difficulté de mener à bien ce blocage. Introduisant un débat sur l'internet et les libertés fondamentales, tenu dans l'hémicycle à la demande du groupe écologiste, Mme Fleur Pellerin, alors ministre déléguée chargée de l'économie numérique nous a répondu très clairement qu'il n'y aurait jamais de décret d'application de cet article. Or, quand une difficulté technique dure plus de quatre ans, c'est qu'il s'agit d'un peu plus que d'une difficulté technique.

J'ai également eu un débat croisé avec les ministres et les parlementaires sur la doctrine du Gouvernement en matière de blocages administratifs. Peut-on confier à des entreprises privées un rôle de police qui est une attribution de l'État régalien ? Le passage par l'autorité judiciaire est nécessaire pour l'ensemble de ces questions. C'est la position que l'opposition soutenait lors de la discussion des lois LOPPSI et j'ai le souvenir des interventions enflammées de Mme Sandrine Mazetier défendant le recours à l'autorité judiciaire.

Sans *a priori* sur la lutte contre le terrorisme, force est de constater que des efforts financiers au profit des cyberpatrouilles sont nécessaires, et parfois plus efficaces que des dispositifs aujourd'hui impossibles ou susceptibles de remettre en cause nos libertés et l'État de droit.

M. Jean-Frédéric Poisson. C'est un exercice assez couru que l'opposition, défendant une proposition de loi devant la commission compétente, reçoive d'abord un satisfecit chaleureux avant d'entendre le ministre expliquer que toutes les mesures proposées figureront dans un texte qui arrivera bientôt – c'est-à-dire plus tard.

Je partage les interrogations de Mme Bechtel sur la sécurité juridique de la notion de « consultation habituelle » et son souhait d'assurer cette sécurité, mais n'est-ce pas précisément ce que permettrait la navette parlementaire ? Il conviendrait donc d'adopter cette proposition de loi en première lecture et d'en sécuriser les dispositions au fil de nos échanges avec le Sénat. Cela serait en outre particulièrement souhaitable compte tenu de la densité du calendrier parlementaire.

En deuxième lieu, je tiens à insister sur la responsabilité des fournisseurs d'accès. L'un des motifs pour lesquels je n'avais, à titre personnel, pas voté la loi Hadopi lors de la précédente mandature était précisément l'absence de cette notion. Or, la seule manière technique de régler le problème que vous soulevez,

monsieur le rapporteur, est précisément de responsabiliser ces opérateurs. Si les fournisseurs d'accès n'agissent pas, le législateur et les forces de l'ordre passeront leur temps à courir, sans les rattraper, après ceux qui inventent des technologies nouvelles. L'article 1er de la proposition de loi est donc particulièrement précieux.

Enfin, le président Bartolone ayant créé voici quelques jours une commission consacrée aux libertés fondamentales et à internet, je tiens à souligner l'ampleur croissante que prend le phénomène de l'usurpation d'identité sur les réseaux numériques. Ce problème doit être réglé, sinon techniquement, du moins juridiquement, afin de réduire les risques pour les citoyens.

Je conclus en rappelant que je suis de ceux qui souhaitent que cette proposition de loi soit adoptée et que la navette parlementaire permette de lui apporter toute la sécurité juridique nécessaire.

Mme Nathalie Kosciusko-Morizet. Je suis heureuse que ce texte figure à l'ordre du jour de notre Assemblée et je veux plaider pour sa prise en compte rapide, sans que l'on doive attendre un texte ultérieur. Le débat n'est pas nouveau, il a longtemps mûri, il faut désormais qu'il trouve rapidement son aboutissement.

La proposition de loi reprend l'esprit des amendements que nous avions déposés en novembre 2012 sur le projet de loi relatif à la sécurité et à la lutte contre le terrorisme, cosignés par une soixantaine de députés parmi lesquels les auteurs de la présente proposition de loi. Le ministre de l'Intérieur de l'époque avait affirmé en commission des Lois être « très ouvert » à ces propositions. En séance publique, il avait confirmé à demi-mot que son avis défavorable devait s'interpréter seulement comme l'effet d'un arbitrage interministériel qu'il n'avait pas remporté. Comme il est aujourd'hui Premier ministre, il sera peut-être plus à même de faire les arbitrages en faveur de cette proposition de loi. La présence parmi nous du nouveau ministre de l'Intérieur est également de bon augure.

De tels sujets doivent dépasser les clivages politiques. Depuis des années que nous travaillons sur ces questions – dont je ne méconnais pas, pour autant, les difficultés techniques et juridiques –, il est maintenant temps d'avancer.

Je l'ai constaté en tant qu'élue locale, certaines familles sont démunies face à l'auto-radicalisation de leurs enfants – conséquence d'une fréquentation assidue des sites faisant l'apologie du terrorisme – et ne savent pas vers qui se tourner.

Dans la mesure où les sites sont hébergés à l'étranger, il n'existe pas de moyen technique simple pour en interdire l'accès. De plus, la notion de consultation régulière ne fait l'objet d'aucune qualification juridique. Néanmoins, les propositions que nous faisons depuis deux ans apportent une réponse opérationnelle. Elles ne résolvent pas tous les problèmes, certes, mais elles donnent les moyens d'identifier les comportements inquiétants et, le cas échéant, de les poursuivre. Bref, ce texte est un outil supplémentaire et nous ne devons nous priver d'aucun outil dans la lutte contre le terrorisme.

Très attachée à la garantie des droits des citoyens sur l'internet, je m'étais inquiétée de certaines dispositions de la loi de programmation militaire permettant à l'État de collecter des données sur les réseaux de communication sans contrôle du juge et sans autorisation préalable de la Commission nationale de contrôle des interceptions de sécurité. Je crois qu'il est possible de respecter le double impératif de la protection des libertés publiques et de l'utilisation par les autorités de nouveaux outils de lutte contre le terrorisme. Cela nécessite un travail de rédaction extrêmement précis. Nous devons veiller à ce que toutes les mesures non conventionnelles – telles que le blocage de sites ou, plus encore, les cyberpatrouilles – restent bien circonscrites au champ particulier de la lutte contre le terrorisme. Les entraves institutionnelles à la vie privée et à la liberté d'expression doivent être strictement limitées aux objets pour lesquelles elles sont nécessaires. Le rapporteur, je le sais, est très attentif à ces questions.

M. Jacques Bompard. Cette proposition de loi a trait à un problème gravissime. Pour une fois, ce n'est pas un texte redondant avec le droit existant. Si, comme l'ensemble de mes collègues, j'approuve pleinement les dispositions qu'il contient, je veux souligner aussi qu'il s'agit d'un traitement symptomatique : il s'agit de traiter, non pas les causes, mais les symptômes de la maladie. C'est bien, mais ce n'est pas en traitant les symptômes que l'on traitera la maladie !

La maladie, c'est qu'il existe dans notre pays – comme dans tous les pays du monde, d'ailleurs – certaines personnes qui ont la haine de la société dans laquelle ils vivent. J'y vois le signe de la mauvaise santé morale et éthique de notre civilisation. En quelque sorte, nous sommes la cause de la maladie qui nous frappe. C'est pourquoi nous devrions faire retour sur ce qu'est notre civilisation, sur ses immenses atouts, et sur la manière dont nous les défendons et les transmettons à l'ensemble de la société.

Le terrorisme naît du communautarisme. L'objectif est donc de supprimer les communautarismes, dont la multiplication actuelle accroît le risque terroriste. Je ne prétends pas avoir de réponse, mais je pense qu'il faut poser la question. Si on ne cherche pas des solutions, il est certain qu'on n'en trouvera pas. Alors, quoi que nous fassions contre le terrorisme, celui-ci continuera de se développer.

M. Lionel Tardy. Cette proposition de loi part d'un constat : le recrutement des djihadistes par internet est un fait, tout comme l'est le recrutement des djihadistes en prison ou ailleurs. J'invite le Gouvernement à traiter le problème globalement. Reste à savoir s'il est nécessaire de passer par une loi !

En l'occurrence, je comprends la volonté de bien faire de mes collègues mais je me pose quelques questions d'ordre technique, les mêmes depuis que nous traitons de ces sujets.

Premièrement, comme on l'a dit lors du débat sur la loi Hadopi, il existe de nombreux moyens de contourner les dispositifs de blocage des sites – sites miroirs, etc. –, surtout quand ceux-ci sont situés à l'étranger.

Deuxièmement, au-delà des sites, ce sont souvent les réseaux sociaux que les terroristes choisissent comme vecteurs de communication. Or ce texte ne les mentionne pas. Dans une logique d'efficacité, monsieur le ministre, ne conviendrait-il pas de privilégier la coopération avec les autorités et les sites américains ? Le blocage des sites internet ne correspond qu'à une partie minime du problème !

M. Éric Ciotti. Ayant cosigné le texte, je ne reviendrai pas sur l'excellente démonstration qu'a faite Guillaume Larrivé de l'utilité du dispositif proposé. Je ne reviendrai pas non plus sur la question, débattue lors de l'examen de la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2) dont j'étais le rapporteur, du blocage par les fournisseurs d'accès de la consultation des sites pédopornographiques, qui présente une similitude avec l'objet de ce texte.

Je pense, monsieur le ministre, qu'il serait préférable que notre proposition de loi soit adoptée, mais j'entends bien vos arguments en faveur d'un examen dans le cadre d'un prochain texte.

Les événements récents doivent nous mobiliser dans un esprit d'unité nationale. Il faut exclure toute polémique. Lors de l'affaire Merah, j'avais trouvé choquantes les prises de position de certains responsables socialistes, y compris M. Hollande – nous étions à quelques jours de l'élection présidentielle –, qui avaient quelque peu brisé l'unité nationale.

Aujourd'hui, le débat est ouvert sur la création d'un fichier d'enregistrement des passagers aériens – *Passenger name record* –, sur le modèle de ce qui existe déjà dans certains pays. Alors qu'actuellement on n'enregistre les passagers qu'au moment de l'embarquement effectif et non au moment de la réservation, les services de renseignement soulignent l'utilité que pourrait avoir un tel outil. Quelle est votre position à ce sujet ?

Par ailleurs, on me dit que la présence d'officiers de liaison entre la DGSE (direction générale de la sécurité extérieure) et la DGSI (direction générale de la sécurité intérieure) n'est plus assurée, ce qui altère le lien entre ces deux administrations alors qu'elles devraient être en dialogue permanent.

Enfin, il semblerait que les fiches « S » ne sont pas toutes consultées par les services de police, notamment par ceux de la police aux frontières.

M. le ministre. Nous sommes tous conscients de l'urgence, monsieur Goujon. Les interrogations que nous formulons au sujet de la proposition de loi ne sont pas de diversion : ce sont des interrogations pragmatiques dictées par notre souci d'être efficaces le plus vite possible. Les éléments sur lesquels nous estimons devoir compléter notre arsenal législatif sont en cours de finalisation. Ils seront présentés en urgence au conseil des ministres et je souhaite qu'ils soient débattus au Parlement dans les meilleurs délais. Ainsi, nous pourrons mobiliser la totalité des outils législatifs dans notre lutte contre le terrorisme.

Comme beaucoup d'entre vous, je souhaite que l'adoption de ces dispositions fasse l'objet de la plus grande unité possible. Les démocraties ne s'arment pas face au terrorisme dans la division, dans la polémique et dans les antagonismes politiques classiques.

De nombreuses questions portent sur l'efficacité réelle des mesures de blocage de sites. Nous connaissons tous les limites techniques de tels dispositifs : dès que l'on bloque un site, un site miroir peut être immédiatement déployé. L'adversaire possède une grande vélocité et une grande capacité d'adaptation, qui justifie d'ailleurs que nous nous adaptions nous-mêmes en permanence : nous faisons face à une menace très différente de celles auxquelles nous avons été confrontés jusqu'à présent.

Cela étant, nous devons tout de même examiner le sujet. Nous avons en effet engagé, à la suite de la réunion qui s'est tenue à Bruxelles le 8 mai dernier avec mon homologue belge Joëlle Milquet, une action résolue au plan européen, et nous nous réunirons de nouveau demain avec nos collègues européens pour discuter des actions à mener à l'égard des fournisseurs d'accès à internet. Si l'Union européenne parvient, en liaison avec les États-Unis, à mener une démarche auprès des grands opérateurs pour les sensibiliser aux risques qui s'attachent à la diffusion d'images, de vidéos et d'éléments de propagande sur internet, notre action sera plus efficace que celle que nous avons menée jusqu'à présent et la question du blocage des sites se posera en d'autres termes. Des expertises et des analyses fines sont nécessaires. Nous en disposerons au moment de la présentation du projet de loi.

S'agissant du décret d'application de l'article 6 de la loi pour la confiance dans l'économie numérique, permettant le blocage des sites pédopornographiques, les travaux se poursuivent. L'Union européenne nous invite à mettre en œuvre le dispositif mais le Conseil constitutionnel a exigé que les opérateurs bénéficient d'une compensation des coûts occasionnés par cette mise en œuvre. Il convient dès lors de limiter strictement le champ de cette compensation afin d'éviter le risque de surcompensation.

Sur « le fait de consulter de façon habituelle » des sites faisant l'apologie du terrorisme, le Conseil constitutionnel et le Conseil d'État se sont en réalité déjà prononcés. Dans son avis sur le projet de loi renforçant la prévention et la répression du terrorisme, le second avait jugé inconstitutionnelle cette disposition sans précédent dans notre législation et sans équivalent dans les autres États membres de l'Union européenne. Si je souhaite que l'on prenne des précautions juridiques en la matière, ce n'est pas par pusillanimité ou par inconscience de l'importance de la question, c'est parce que je pense que nous devons être forts. Or, chaque fois que nous légiférons en prenant le risque de nous faire casser, nous nous affaiblissons dans le combat que nous menons. Je n'ai pas d'états d'âme quant à la nécessité d'atteindre le but : c'est au contraire parce que j'ai l'obsession de l'atteindre que je ne souhaite pas que nous nous exposions à voir nos dispositions législatives remises en cause par le Conseil constitutionnel ou le

Conseil d'État. Je propose donc que nous prenions le temps de travailler ensemble pour être sûrs que la cible sera atteinte.

Il est exact, monsieur Coronado, que nous disposons déjà d'outils nombreux pour lutter contre le terrorisme. Mais, en l'espèce, la menace est d'une autre nature. Nous sommes confrontés à des gens qui font muter en permanence leurs modalités d'action et de réaction. Sur certains sites internet, on explique même les méthodes de dissimulation permettant d'échapper à tous les dispositifs de contrôle. Face à cette menace mouvante, face à ces acteurs qui s'adaptent en permanence pour nous frapper, nous devons compléter et adapter nous aussi notre arsenal législatif. Par exemple, lorsqu'il existe un faisceau de présomptions laissant penser qu'une personne majeure pourrait rejoindre un théâtre d'opérations djihadiste, nous n'avons pas la possibilité juridique de nous opposer à son départ si elle ne fait pas l'objet d'un contrôle ou d'une procédure judiciaires. De même, l'intervention sous pseudonyme, qui améliore l'efficacité des patrouilles sur internet, doit être renforcée.

Bref, il ne s'agit pas de « jouer la montre » mais au contraire de présenter rapidement un texte offrant toutes les garanties juridiques et de l'alimenter par toutes les réflexions parlementaires.

Je voudrais conclure mon propos en évoquant une affaire qui provoque mon indignation.

Le combat dans lequel nous sommes engagés est difficile. Il exige vérité et rigueur intellectuelle de la part de tous ceux qui y prennent part, notamment les membres de l'exécutif. C'est ce qui me conduit à me présenter devant vous aujourd'hui. Les commissions parlementaires pourront m'entendre aussi souvent qu'elles le voudront lorsqu'elles auront besoin d'explications – en veillant, bien entendu, à ce que rien n'altère l'efficacité des actions engagées par nos services.

Mais cette responsabilité doit être partagée. Or, hier soir, le site du *Nouvel Observateur* a publié un article indiquant une « grave erreur » des services de renseignement dans la surveillance de Mehdi Nemmouche pouvait être à l'origine des crimes perpétrés à Bruxelles. L'article a été repris par d'autres sites d'information, notamment belges, et relayé sur Twitter.

Avant d'aller me recueillir cet après-midi, avec mon homologue belge, au musée juif de Bruxelles, je veux ici rétablir les faits. Dès sa sortie de prison, en décembre 2012, Mehdi Nemmouche a fait l'objet d'une « mise en attention Schengen » par la DGSI. Cette fiche donna d'ailleurs lieu à un signalement, le 18 mars 2014, par les autorités allemandes, qui indiquèrent l'arrivée de l'intéressé sur leur territoire en provenance de Bangkok. À notre connaissance, l'oncle de Mehdi Nemmouche, auquel l'article fait allusion, demeure à l'étranger et ne fait l'objet d'aucune incrimination en matière pénale ou de terrorisme.

Je veux donc rappeler chacun à ses responsabilités. Lorsque l'on met en cause, par des informations fausses et des amalgames, des services de

renseignement qui font leur travail, on porte atteinte à l'image de notre pays et au combat qu'il mène.

Je suis très attaché à la liberté de la presse. Je rendrai compte à la presse du fonctionnement de mon ministère aussi souvent qu'elle le voudra. Mais je n'accepterai jamais que l'on mette en cause par de telles contrevérités les agents et les services qui sont sous ma responsabilité, sans même prendre la peine de les appeler pour vérifier les informations. Cela est de nature à nuire aux intérêts de notre pays. Liberté et responsabilité sont étroitement liées, et toute personne qui écrit ou qui porte une parole pouvant être diffusée dans l'espace public a aussi une responsabilité.

Ces éléments me paraissent suffisamment graves pour que je fasse cette mise au point sévère devant votre Commission.

M. le rapporteur. Je remercie le ministre de l'Intérieur non seulement pour sa participation personnelle à nos travaux, mais aussi pour la disponibilité de ses services et pour l'état d'esprit constructif avec lequel il aborde cette proposition de loi.

Je formulerai deux remarques techniques.

Le délit de « consultation habituelle » est une matière délicate, j'en conviens, puisqu'elle appelle le législateur à préserver l'équilibre nécessaire entre les exigences de la sauvegarde de l'ordre public et les exigences afférentes au respect des libertés. J'entends bien que le Conseil d'État, en section administrative, après avoir été saisi au printemps 2012 du projet de loi de M. Mercier, avait exprimé certaines réserves. Toutefois, la Cour de cassation, saisie d'une disposition pénale très voisine, celle du délit de consultation habituelle de sites pédopornographique, a estimé en juin 2012 qu'il n'était pas nécessaire de saisir le Conseil constitutionnel d'une question prioritaire de constitutionnalité. Les positions des deux cours suprêmes de l'ordre administratif et de l'ordre judiciaire sont donc très différentes.

Je crois qu'il appartient à chacun de prendre ses responsabilités – après, le cas échéant, une amélioration rédactionnelle qui peut toujours intervenir lors de la navette – et que le législateur est fondé à intervenir, sous réserve, naturellement, de l'examen réalisé *a posteriori* par le Conseil constitutionnel.

Concernant maintenant le blocage des sites, je retiens de votre intervention, monsieur le ministre, que le principal obstacle que vous identifiez à ce stade est moins d'ordre juridique que d'ordre financier. Nous ne pouvons qu'encourager le Gouvernement à « mettre la pression » sur les fournisseurs d'accès à internet, qui nous sont apparus, lors des auditions, particulièrement timorés sur toutes ces questions et peut-être insuffisamment sensibles aux devoirs qui leur incombent en matière d'intérêt général.

Je remercie mes collègues Goujon, Poisson, Kosciusko-Morizet et Ciotti pour leur soutien et pour l'accent qu'ils mettent sur la nécessité d'avancer dans l'intérêt même de la protection des mineurs.

Nous sommes ouverts, madame Bechtel, à toute amélioration technique et juridique que vous pourriez suggérer par voie d'amendement.

Je sais, monsieur Coronado, que vous tenez à l'intervention d'un juge judiciaire dans ces matières. Mais, là encore, ce n'est pas une exigence constitutionnelle. Lorsque le Conseil Constitutionnel a été saisi, en 2011, du dispositif de blocage des sites pédopornographiques, il a jugé que devait être écartée l'objection selon laquelle le contrôle par le juge judiciaire était nécessaire en ces matières. Même en matière de police administrative, il y a toujours possibilité pour le juge administratif d'intervenir de manière urgente par la voie du référé.

Dans notre esprit, monsieur Tardy, la proposition de loi couvre le champ des réseaux sociaux. Pour autant qu'ils soient accessibles au public, ce sont bien des « services de communication au public en ligne ».

Chacun ici en est convaincu : la procrastination n'est pas une solution. Je forme donc le vœu que cette proposition de loi prospère. Et si elle devait être rejetée, nous participerions activement au débat sur le projet de loi annoncé.

La Commission en vient à l'examen des articles de la proposition de loi.

EXAMEN DES ARTICLES

Article 1er

(art. 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique)

Surveillance des sites internet faisant l'apologie du terrorisme et blocage de l'accès à ces sites

Cet article vise à introduire deux nouveaux outils de lutte contre les sites internet faisant l'apologie du terrorisme. D'une part, il renforce les obligations de surveillance pesant sur les acteurs de l'internet. D'autre part, il permet le blocage de l'accès à certains sites faisant l'apologie du terrorisme, dont la liste serait arrêtée par le ministre de l'Intérieur.

1. Le renforcement des obligations de surveillance des fournisseurs d'accès à internet et des hébergeurs de sites

L'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) définit les principales règles juridiques en matière de régulation des contenus sur internet et le rôle des différents acteurs, notamment les fournisseurs d'accès et les hébergeurs de sites.

Le principe posé à cet article est que les fournisseurs d'accès et les hébergeurs ne sont pas responsables – ni pénalement, ni civilement – des contenus des sites internet auxquels ils permettent l'accès ou qu'ils hébergent. Ils ne sont pas davantage soumis « *à une obligation générale de surveiller les informations qu'[ils] transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites* » [(1)].

Toutefois, la loi leur impose **certaines obligations de vigilance spécifiques, visant à lutter contre certains types de criminalité**. En particulier, en application du troisième alinéa du 7 du I de l'article 6 précité, les fournisseurs d'accès et les hébergeurs doivent, au nom de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale, de la pornographie enfantine, de l'incitation à la violence (notamment faite aux femmes) et des atteintes à la dignité humaine, « *concourir à la lutte contre la diffusion* » sur internet de certaines infractions.

---

(1) Premier alinéa du 7 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée. En revanche, les hébergeurs peuvent voir leur responsabilité engagée s'ils n'ont pas réagi avec promptitude pour retirer des données ou en rendre l'accès impossible, dès lors qu'ils ont eu la connaissance effective de leur caractère illicite (3 à 5 du I du même article). Le Conseil constitutionnel a précisé que « ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge *» (décision n° 2004-496 DC du 10 juin 2004,* Loi pour la confiance dans l'économie numérique*).*

Il s'agit des infractions suivantes [1] :

– l'apologie de crimes contre l'humanité, de crimes de guerre et d'autres crimes mentionnés au cinquième alinéa de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse ;

– la provocation à la discrimination, à la haine ou à la violence contre des personnes en raison de leur origine, de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée (huitième alinéa du même article 24) :

– la diffusion d'images pédopornographiques, punie par l'article 227-23 du code pénal [2] ;

– la diffusion de message à caractère violent, pornographique ou portant gravement atteinte à la dignité humaine et susceptible d'être vu ou perçu par un mineur, réprimée par l'article 227-24 du même code.

Signalons que l'article 17 du projet de loi pour l'égalité entre les femmes et les hommes, en cours de discussion au Parlement, tend à étendre le champ de ce dispositif aux infractions de provocation à la haine ou à la violence contre des personnes en raison de leur sexe, de leur orientation ou leur identité sexuelle ou de leur handicap (neuvième alinéa de l'article 24 de la loi de 1881) et au délit de diffusion d'images de violence défini à l'article 222-33-3 du code pénal (« *happy slapping* ») [3]. Signalons également que l'article 1er de la proposition de loi renforçant la lutte contre le système prostitutionnel, en instance d'examen par le Sénat, vise à ajouter, parmi les infractions devant faire l'objet d'un signalement par les fournisseurs d'accès à internet et les hébergeurs de sites celles prévues aux articles 225-4-1 (traite des êtres humains), 225-5 et 225-6 (proxénétisme) du code pénal.

Afin de lutter contre les différentes infractions qui précèdent, le quatrième alinéa du 7 du I de l'article 6 de la loi du 21 juin 2004 précitée **met à la charge des fournisseurs d'accès et des hébergeurs trois types d'obligations** [4] :

– ils doivent « *mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance* » ce type de données

---

(1) Un système comparable, mais moins contraignant pour les fournisseurs d'accès et les hébergeurs, existe également pour réprimer les activités illégales de jeux d'argent sur internet (avant-dernier alinéa du 7 du I du même article 6).

(2) Sur cet article, voir également infra *le commentaire de l'article 2 de la présente proposition de loi.*

(3) Le « happy slapping *» – ou « vidéoagression » – consiste à filmer, en vue de sa diffusion, l'agression physique d'une personne, généralement à l'aide d'un téléphone portable ou d'un smartphone.*

(4) En application du VI du même article 6, le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une société de fourniture d'accès ou d'hébergement, de ne pas satisfaire à ces obligations est puni d'un an d'emprisonnement et de 75 000 euros d'amende. Les personnes morales déclarées pénalement responsables encourent, outre l'amende dont le montant maximal est fixé à 375 000 euros en application de l'article 131-38 du code pénal, les peines complémentaires prévues aux 2° à 9° de l'article 131-39 du code pénal, notamment l'interdiction d'exercer, pour une durée de cinq ans au plus, l'activité professionnelle dans l'exercice ou à l'occasion de laquelle l'infraction a été commise.

illicites. Les internautes peuvent ainsi, par exemple, signaler un contenu jugé illégal ou choquant sur le site http://www.pointdecontact.net, géré par l'Association des fournisseurs d'accès et de services internet (AFA), qui regroupe fournisseurs d'accès, hébergeurs, moteurs de recherche et diverses plateformes numériques. C'est également sur le fondement de cette disposition que *Twitter* s'est vu ordonner par le tribunal de grande instance de Paris, en référé, « *de mettre en place dans le cadre de la plateforme française du service Twitter, un dispositif facilement accessible et visible permettant à toute personne de porter à sa connaissance des contenus illicites, tombant notamment sous le coup de l'apologie de crime contre l'humanité et de l'incitation à la haine raciale* » (1) ;

– ils ont l'obligation « *d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services* » ;

– ils doivent « *rendre publics les moyens qu'*[ils] *consacrent à la lutte contre ces activités illicites* ».

En pratique, les signalements de contenus illicites par les fournisseurs d'accès et par les hébergeurs sont effectués auprès de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), qui relève de la direction centrale de la police judiciaire du ministère de l'Intérieur.

Ce service gère une plateforme en ligne de signalement, dénommée « PHAROS » (plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements), accessible sur le site http://www.internet-signalement.gouv.fr. Ce dispositif vise à recueillir, de manière centralisée, l'ensemble des signalements (par les utilisateurs comme par les professionnels d'internet), à procéder à des rapprochements entre eux et à les orienter vers les services enquêteurs compétents, en vue de leur exploitation. En 2012, 120 000 signalements ont ainsi été adressés à ce service (après 100 000 en 2011 et 77 000 en 2010), dont 1 329 ont été transmis à la police nationale et 3 970 confiés à Interpol pour enquête (2). Selon les informations recueillies par votre rapporteur auprès de Mme Valérie Maldonado, directrice de l'OCLCTIC, le nombre de signalements a encore progressé en 2013, atteignant près de 124 000.

Le **1°** du présent article tend **à élargir ce dispositif de vigilance, reposant sur les acteurs de l'internet, à la répression de l'apologie du terrorisme**.

Compte tenu du nombre d'infractions aujourd'hui concernées par les obligations pesant sur les fournisseurs d'accès et sur les hébergeurs, on ne peut que s'étonner de ce que l'apologie du terrorisme ne figure pas parmi les infractions concernées. On relèvera d'ailleurs que le site « point de contact » précité, mis en place par les principaux fournisseurs d'accès et hébergeurs, permet

(1) Tribunal de grande instance de Paris, 24 janv. 2013, Twitter c./ Union des étudiants juifs de France.

(2) Étude d'impact jointe au projet de loi pour l'égalité entre les femmes et les hommes.

d'ores et déjà aux internautes, *praeter legem*, de signaler des contenus portant « *provocation au terrorisme et à la fabrication de bombes* » [(1)].

Le **1°** du présent article va cependant plus loin, **en obligeant les fournisseurs d'accès à internet et les hébergeurs de sites à signaler aux autorités les sites faisant l'apologie du terrorisme**, au sens du sixième alinéa de l'article 24 de la loi de 1881 précitée [(2)]. Rappelons que ce dernier punit de cinq ans d'emprisonnement et de 45 000 euros d'amende ceux qui, par voie de presse ou par tout autre moyen de publication [(3)], « *auront provoqué directement aux actes de terrorisme prévus par le titre II du livre IV du code pénal, ou qui en auront fait l'apologie* ».

Cette mesure, qui ne ferait qu'élargir le champ d'un dispositif déjà existant, ne représenterait pas une charge considérable pour les acteurs de l'internet. L'enjeu n'est cependant pas négligeable, si l'on en juge par **l'augmentation, ces dernières années, du nombre de signalements par les internautes, auprès de la plateforme PHAROS, de sites faisant l'apologie du terrorisme**. Selon les indications fournies par Mme Valérie Maldonado, alors que seulement 13 signalements de ce type avaient été enregistrés en 2011, ce nombre a été porté à 120 en 2012, puis à 360 en 2013 – soit **près d'un signalement pour apologie du terrorisme par jour**. En 2013, les principaux sites concernés par ces signalements ont été les réseaux sociaux (en particulier *Facebook* et *Twitter*), qui représentaient 54 % du total, suivis de blogs (14 %), de sites internet thématiques (13 %), de *Youtube* (6 %), de forums (6 %) et de divers autres sites (7 %).

2. Le blocage de l'accès à certains sites internet faisant l'apologie du terrorisme

Au-delà du renforcement de la surveillance des sites faisant l'apologie du terrorisme, le **2°** du présent article tend à permettre le blocage de l'accès aux plus menaçants d'entre eux pour l'ordre public.

En effet, le caractère transnational de la cybercriminalité fait que, en dépit des moyens offerts par le droit en vigueur [(4)], le signalement auprès des autorités, par un fournisseur d'accès ou un hébergeur, d'un contenu illicite n'offre aucune garantie quant à la possibilité d'obtenir la *fermeture* rapide du site concerné et *a fortiori* la poursuite et la condamnation de ses concepteurs. Le dispositif proposé

---

(1) http://www.pointdecontact.net/provocation_au_terrorisme_et_a_la_fabrication_de_bombes

(2) Pour plus de clarté, il conviendrait d'ailleurs de mentionner cette disposition au 1° du présent article, plutôt que de procéder au renvoi à l'apologie « des crimes visés par les articles 421-1 à 421-2-2 du code pénal ».

(3) Y compris un « moyen de communication au public par voie électronique » *(article 23 de la loi de 1881 précitée).*

(4) En particulier, le 8 du I de l'article 6 de la loi du 21 juin 2004 précitée permet à l'autorité judiciaire de prescrire, en référé ou sur requête, aux hébergeurs ou, à défaut, aux fournisseurs d'accès, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne.

permettrait à tout le moins, à la demande des pouvoirs publics, d'empêcher l'*accès* à de tels sites.

a. Le précédent de la lutte contre la pédopornographie

C'est le même raisonnement qui a prévalu en matière de lutte contre la pédopornographie en 2011 : partant du principe que la très grande majorité des images de pornographie enfantine sont diffusées sur internet par des sites hébergés à l'étranger, à l'égard desquels il est juridiquement difficile d'agir, **le législateur a, dans la « LOPPSI 2 », introduit un mécanisme spécifique de blocage des sites pédopornographiques** (1).

L'article 6 de la loi du 21 juin 2004 précitée a été complété, pour prévoir que « *lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux [fournisseurs d'accès à internet] les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai* » (2).

Le ministre de l'Intérieur peut ainsi dresser une « liste noire » de sites jugés particulièrement pernicieux et obtenir des fournisseurs d'accès à internet qu'ils « coupent » l'accès à de tels sites. Concrètement, ces sites existent toujours, mais ne sont plus accessibles aux internautes français. L'utilisateur qui cherche à s'y connecter aboutit à une page *web* l'informant du caractère illicite du site auquel il tentait d'accéder.

De tels mécanismes de blocage existent d'ores et déjà en Norvège, en Suède et au Danemark (*Child Abuse Anti Distribution Filter*).

Le dispositif prévu dans la LOPPSI 2 a été jugé conforme à la Constitution par le Conseil constitutionnel, ce dernier soulignant en particulier :

– qu'il n'aboutissait pas à priver les utilisateurs de tout accès à internet, mais seulement à conférer « *à l'autorité administrative le pouvoir de restreindre, pour la protection des utilisateurs d'internet, l'accès à des services de communication au public en ligne lorsque et dans la mesure où ils diffusent des images de pornographie infantile* » ;

– que la décision de l'autorité administrative était « *susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé* » (3).

---

(1) Article 4 de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2).

(2) Cinquième alinéa du 7 du I de l'article 6 de la loi du 21 juin 2004 précitée.

(3) Décision n° 2011-625 DC du 10 mars 2011, Loi d'orientation et de programmation pour la performance de la sécurité intérieure.

Le Conseil constitutionnel en avait conclu que les dispositions en cause assuraient « *une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789* ».

Il faut toutefois regretter que, plus de trois ans après le vote de la LOPPSI 2, ce dispositif ne soit toujours pas en vigueur, faute pour le Gouvernement d'avoir pris le décret définissant les modalités techniques retenues pour que les fournisseurs d'accès procèdent au blocage des sites pédopornographiques, ainsi que la compensation financière qui leur est due (1).

Ces deux questions sont d'ailleurs liées : les dispositifs techniques qui permettent de bloquer le plus « finement » les sites concernés – c'est-à-dire sans empêcher l'accès à d'autres sites parfaitement licites – sont aussi les plus coûteux pour les fournisseurs d'accès (2).

Plusieurs parlementaires se sont déjà préoccupés de la mise en œuvre de ce dispositif. Dès le mois d'août 2012, le soussigné appelait l'attention du ministre de l'Intérieur sur l'application de la LOPPSI 2 (3). En février 2013, M. Jean-Luc Warsmann, ancien président de votre Commission, s'inquiétait de ce que la mesure de blocage des sites pédopornographiques ne soit toujours pas entrée en vigueur (4).

Aucun décret n'étant intervenu depuis lors, l'obligation pour les fournisseurs d'accès d'empêcher les internautes d'accéder aux sites diffusant des images de pédopornographie demeure purement virtuelle (5). Le 29 novembre 2013, Mme Najat Vallaud-Belkacem, ministre des Droits des femmes, porte-parole du Gouvernement, indiquait même à l'Assemblée nationale : « *Je ne vous cache pas que le Gouvernement s'interroge sur l'adoption de ce décret* » (6).

---

(1) Le sixième alinéa du 7 du I de l'article 6 de la loi du 21 juin 2004 précitée dispose : « Un décret fixe les modalités d'application de l'alinéa précédent, notamment celles selon lesquelles sont compensés, s'il y a lieu, les surcoûts résultant des obligations mises à la charge des opérateurs ».

*(2) La solution techniquement la plus efficace consiste à procéder au blocage au niveau de l'URL (*Uniform Resource Locator*), c'est-à-dire au niveau de l'adresse de la page* web *concernée. Au contraire, un blocage au niveau de l'adresse IP (*Internet Protocol*, numéro d'identification attribué à chaque appareil connecté à internet) risque de toucher également des contenus licites («sur-blocage »), compte tenu de la difficulté technique qu'il y a à connaître de façon exhaustive les sites correspondant à une même adresse IP. Entre ces deux dispositifs, le blocage au niveau du nom de domaine apparaît comme une solution médiane.*

(3) Question n° 2747, JO *du 7 août 2012, p. 4671 ; réponse publiée au* JO *du 9 octobre 2012, p. 5573.*

(4) Question n° 17415, JO *du 5 février 2013, p. 1239 ; réponse publiée au* JO *du 7 mai 2013, p. 5026.*

(5) Si un arrêté ministériel du 3 octobre 2013 ajoute les fournisseurs d'accès à internet à la liste des possibles destinataires des données contenues dans la plateforme PHAROS précitée, cette modification est sans aucun lien avec la question de la pédopornographie : elle vise à lutter contre les escroqueries commises sur internet au moyen de fausses adresses e-mail *(arrêté du 3 octobre 2013 modifiant l'arrêté du 16 juin 2009 portant création d'un système dénommé « PHAROS » [plate-forme d'harmonisation, d'analyse de recoupement et d'orientation des signalements]).*

(6) Deuxième séance du 29 novembre 2013.

Le 11 mars 2014, le ministre de l'Intérieur indiquait pourtant, en réponse à une question écrite [(1)], que « *les conditions de mise en œuvre* » de cette mesure faisaient « *l'objet d'une réflexion dans le cadre du groupe de travail interministériel sur la cybercriminalité* », présidé par M. Marc Robert, procureur général près la cour d'appel de Riom. Régulièrement annoncé, le rapport de ce groupe de travail n'est toujours pas disponible [(2)].

b. La transposition aux sites faisant l'apologie des actes de terrorisme

S'inspirant des dispositions applicables à la pédopornographie, le **2°** du présent article ouvre la possibilité de **bloquer l'accès à des sites internet qui diffusent des images ou des représentations faisant l'apologie des actes de terrorisme** prévus par le titre II du livre IV du code pénal, c'est-à-dire l'ensemble des actes punis par les articles 421-1 à 421-6 [(3)].

Ce sont les fournisseurs d'accès à internet [(4)] qui auraient l'obligation d' « *empêcher l'accès sans délai* » à certains sites internet, non pas de leur propre initiative, mais à la demande des autorités chargées de lutter contre le terrorisme.

C'est donc aux services du ministère de l'Intérieur qu'il reviendra d'identifier les contenus illicites et de les signaler aux fournisseurs d'accès à internet. **Concrètement, la « liste noire » des sites qu'il convient de bloquer leur serait notifiée par le ministre de l'Intérieur, l'OCLCTIC transmettant par voie dématérialisée les données techniques nécessaires**. Dans les cas les plus nombreux, en particulier sur les réseaux sociaux, le blocage ne concernerait que certaines *pages* de sites internet.

Votre rapporteur insiste sur le fait que **le blocage des sites ne serait qu'une *faculté* pour le ministère de l'Intérieur** : le dispositif est donc conçu comme un moyen supplémentaire à la disposition des autorités chargées de lutter contre le terrorisme, non comme une mesure générale de filtrage.

L'usage qui serait fait de ce nouvel outil serait donc nécessairement *ciblé* sur certains sites particuliers, sans préjudice de la possibilité de ne pas faire figurer d'autres sites sur cette liste noire, à des fins d'enquête, d'infiltration ou de recueil de renseignements.

---

(1) Question n° 40429, JO *du 22 octobre 2013, p. 10984 ; réponse publiée au* JO *du 11 mars 2014, p. 2434.*

(2) Alors que la lettre de mission date du 17 juin 2013, la remise du rapport a d'abord été annoncée par le Gouvernement pour la fin novembre 2013, puis pour la mi-février 2014. Dans la réponse à la question précitée, soit en mars 2014, le ministère de l'Intérieur indique que le groupe de travail « rendra ses conclusions prochainement *». Le 22 mai 2014, la réponse se faisait moins affirmative : «* il devrait rendre prochainement ses conclusions *» (réponse à la question de M. Bruno Retailleau, sénateur, n° 10549,* JO *du 22 mai 2014, p. 1206).*

(3) Les infractions prévues par ces articles sont présentées en détail dans le commentaire de l'article 2 de la présent proposition de loi.

(4) C'est à eux que renvoient les dispositions : « les personnes mentionnées au 1 du I *» de l'article 6 de loi du 21 juin 2004 précitée.*

Comme en matière de pédopornographie, ce nouveau dispositif serait potentiellement applicable à **l'ensemble des services de communication au public en ligne**, y compris aux réseaux sociaux.

Plus précisément, entreraient dans son champ d'application :

– les sites internet « classiques » ;

– les plateformes vidéo, comme *Dailymotion* ou *Youtube*, lesquelles sont assimilées par la jurisprudence à des hébergeurs (1) ;

– les réseaux sociaux, tels que *Facebook* (2) ou *Twitter* (3), également considérés comme des hébergeurs ;

– les sites de conversion (*chat*) et les forums de discussion (4) ;

– les sites d'échanges d'internaute à internaute (*peer-to-peer*), ainsi qu'en atteste la jurisprudence en matière de pédopornographie (5).

Le seul obstacle à l'applicabilité du présent article pourrait éventuellement résider dans l'accessibilité limitée de certains de ces sites, qui pourraient alors ne plus être considérés comme servant à la communication « *au public* », mais relever de la correspondance privée. Quoique la jurisprudence en la matière – qui fait parfois preuve d'une subtile casuistique – ne soit pas très fournie, tel pourrait être le cas d'un forum de discussion dont l'entrée serait sévèrement filtrée (6) ou d'une page *Facebook* qui ne serait accessible qu'à un nombre très restreint d'internautes (7).

---

(1) Cour de cassation, civ. 1re, 17 février 2011, n° 09-67.896, Sociétés Nord-Ouest et UGC Image c./ Dailymotion.

(2) Tribunal de grande instance de Paris, référé, 20 avril 2010, Hervé G. c./ Facebook France.

(3) Le caractère public des propos échangés sur Twitter *est consubstantiel au principe même de fonctionnement du site, dont les conditions d'utilisation indiquent : «* Ce que vous dites sur Twitter est visible partout dans le monde instantanément ».

(4) Cour de cassation, crim., 16 février 2010, n° 08-86.301.

(5) Cour d'appel de Rennes, 17 mai 2011, n°11/00411 (échange de fichiers sur Shareaza*) ; cour d'appel d'Amiens, 16 janvier 2009, n° 08/00114 et cour d'appel de Montpellier, 17 mars 2011, n°10/01099 (échange de fichiers sur* Kazaa*).*

(6) Tribunal de grande instance de Paris, référé, 5 juillet 2002, M. Hubert Marty-Vrayance c./ Sociétés Édition la Découverte et Vivendi Publishing Services *: pour qu'un forum sur internet soit considéré comme privé, l'administrateur du site doit procéder à une sélection des internautes «* fondée sur un choix positif des usagers qui permette d'assurer leur nombre restreint et leur communauté d'intérêt », *au moyen de critères permettant «* de réserver effectivement l'usage du site à certains internautes déterminés, de manière sûre et précise, en fonction de certains éléments, préalablement vérifiés ». *En revanche, «* un simple "filtrage" qui, quelles que soient les mises en garde diffusées sur le site, dépend des seules déclarations des internautes, n'offre aucune garantie sérieuse, quant à l'accès limité du site et demeure, dès lors, en principe, accessible à tous ».

(7) Cour de cassation, civ. 1re, 10 avril 2013, n° 11-19.530 : « attendu qu'après avoir constaté que les propos litigieux avaient été diffusés sur les comptes ouverts par Mme Y... tant sur le site Facebook que sur le site MSN, lesquels n'étaient en l'espèce accessibles qu'aux seules personnes agréées par l'intéressée, en nombre très restreint, la cour d'appel a retenu, par un motif adopté exempt de caractère hypothétique, que celles-ci formaient une communauté d'intérêts ; (…) elle en a exactement déduit que ces propos ne constituaient pas des injures publiques ».

Votre rapporteur souligne, par ailleurs, que **la constitutionnalité du présent article ne fait guère de doutes**, dès lors que le mécanisme de blocage des sites pédopornographiques a, en 2011, expressément été jugé conforme à la Constitution par le juge constitutionnel, dans les conditions précédemment rappelées. En l'occurrence, le dispositif proposé poursuit, par une mesure de police administrative, **l'objectif à valeur constitutionnelle de sauvegarde de l'ordre public**, en évitant que des utilisateurs d'internet ne soient exposés à des images choquantes et que certains esprits influençables ne soient tentés de passer à l'acte. Au total, la prévention de la commission d'actes de terrorisme justifie qu'il soit porté une atteinte non disproportionnée à la liberté de communication garantie par l'article 11 de la Déclaration de 1789 [(1)].

Si d'aucuns ne manqueront pas d'objecter que, comme pour tout dispositif technique, l'interdiction d'accès pourra parfois être contournée (par exemple en créant de nouveaux sites reprenant le même contenu que les sites bloqués ou en mettant en place des sites « miroirs »), celle-ci aurait au moins le mérite de complexifier l'accès d' « apprentis terroristes » à des idées pernicieuses et à des informations dangereuses et, partant, de dissuader les moins motivés d'entre eux.

*

* *

*La Commission est saisie, en présentation commune, des amendement*s *CL1 et CL5 de M. Sergio Coronado.*

M. Sergio Coronado. Ces deux amendements, ainsi que l'amendement CL6, tendent à supprimer tout ou partie de l'article.

Le 1° étend l'obligation faite aux hébergeurs et fournisseurs d'accès à internet (FAI) de mettre en place des dispositifs de signalement des contenus illicites ayant trait au terrorisme. Il ne vise pas à interdire ces contenus, mais seulement à instaurer une obligation spécifique aux FAI et hébergeurs, permettant dès lors d'engager leur responsabilité civile et pénale. Nous avons abordé ce sujet, je l'ai dit, à l'occasion d'autres débats, dont celui sur le texte visant à pénaliser les clients de personnes prostituées.

Je conviens, monsieur le rapporteur, que l'obligation du recours au juge judiciaire n'est pas un principe constitutionnel, mais je rappelle que le Conseil constitutionnel a déjà noté « *la difficulté fréquente d'apprécier la licéité d'un contenu* » pour un hébergeur. Cela me semble particulièrement vrai en matière de terrorisme. Autant, en matière de pédopornographie, il y a peu de place pour l'appréciation subjective, autant il est difficile de discerner si un propos incite à l'engagement terroriste ou fait l'apologie du terrorisme. Il serait périlleux d'en

(1) Laquelle implique « la liberté d'accéder *» aux services de communication au public en ligne, selon le Conseil constitutionnel (décision n° 2009-580 DC du 10 juin 2009,* Loi favorisant la diffusion et la protection de la création sur internet, *cons. 12).*

confier l'appréciation à des entreprises privées qui auraient à décider de ce qui est licite ou non en la matière.

En outre, il me semble un peu hasardeux de multiplier les plateformes. Mieux vaudrait que le signalement de ce type de contenu passe par la plateforme existante PHAROS.

Le 2° de l'article vise à mettre en place un blocage administratif difficilement applicable dans les faits. Juste après le blocage judiciaire du site Copwatch, par exemple, on a découvert trente-cinq sites miroirs.

Concernant les sites pédopornographiques, j'estime que l'absence de publication du décret d'application permettant le blocage administratif n'est pas seulement due, comme l'a suggéré le ministre, à des questions d'ordre financier. S'attaquer concrètement à ces contenus présente une vraie difficulté technique. Les sites en question ne sont pas aisément repérables : il s'agit souvent de sites cryptés de partage de contenus, d'échange de fichiers. On ne les trouve pas par une simple recherche sur Google : ils font appel à des constructions techniques très élaborées et très en pointe.

En outre, l'exemple australien a montré que le blocage administratif manque de finesse et de pertinence, ce qui présente des risques : on a constaté que le dispositif atteignait aussi toute une série de sites annexes ou connexes.

L'Assemblée nationale est un autre bon exemple. En effet, par décision du Bureau, il est interdit d'avoir accès à des sites à caractère pornographique à partir du réseau de l'Assemblée – à l'époque, j'avais trouvé étonnant que l'on décide à la place de personnes majeures et vaccinées ce à quoi elles avaient droit quand elles naviguaient sur internet ! Pour avoir testé le dispositif mis en place, j'ai constaté que l'accès à plusieurs sites d'information et sites militants était bloqué.

Au surplus, de tels blocages hâtifs et peu précis pourraient entraver le bon déroulement des enquêtes en cours.

M. le rapporteur. Avis défavorable pour les raisons de fond déjà exposées mais aussi pour une raison de forme : si l'article était supprimé et le reste de la proposition adopté, cet article ne serait pas débattu dans l'hémicycle, ce qui nuirait au caractère constructif de la discussion à laquelle le ministre de l'Intérieur nous a invités.

Mme Marie-Françoise Bechtel. L'article 1er comporte deux dispositions très hétérogènes.

Le 1° vise à étendre la responsabilité des fournisseurs d'accès aux contenus faisant l'apologie du terrorisme. Cette responsabilité étant déjà exercée dans un domaine plus restreint, la question de la licéité est réglée. La disposition proposée me semble de bon sens et utile. Cela dit, le ministre ayant indiqué qu'il entendait engager une négociation avec l'Union européenne pour peser sur les

fournisseurs d'accès à internet, cet alinéa gagnera, dans le projet de loi annoncé par le Gouvernement, à être affiné dans cette perspective.

Quant au blocage des sites prévu au 2°, on sait que ce n'est pas une mesure très efficace, si tant est qu'on la considère comme opportune. Des juges auditionnés à l'occasion de la discussion de précédents textes nous ont indiqué qu'il était souvent préférable de ne pas bloquer certains sites, de manière à les laisser se développer et à permettre aux enquêteurs de recueillir un faisceau de présomptions.

En d'autres termes, je suis défavorable au 2°, et favorable au 1° sous réserve de plus amples précisions quant à la négociation avec les fournisseurs d'accès. Mieux vaut, dès lors, ne pas adopter les amendements de M. Coronado, afin de nous prononcer sur l'ensemble de la proposition de loi.

M. le président Jean-Jacques Urvoas. Je partage votre point de vue, ma chère collègue.

L'extension de la contrainte imposée aux fournisseurs d'accès est la seule manière de répondre à ce qu'il faut bien appeler leur hypocrisie. Le rapporteur l'a dit et j'en ai aussi fait l'expérience, les FAI se cachent derrière des notions qui n'ont plus lieu d'être. Il suffit de passer deux ou trois filtres sur YouTube pour tomber sur des vidéos de décapitation. Cela signifie qu'avec un minimum d'exigence, les fournisseurs d'accès et hébergeurs ont les moyens d'avoir connaissance de ce qu'ils diffusent. Mais, puisqu'ils continuent de se draper dans leur vertu, arrive un moment où la loi doit les contraindre.

Je suis donc enclin à voter ce dispositif, mais je suis en désaccord avec le reste du texte. L'idée de mettre en place des « cyberpatrouilles » est intéressante, certes, mais les services ont déjà les moyens de faire des infiltrations sous pseudonyme. Ce qui fait craindre un raisonnement *a contrario* si nous adoptions cette disposition : ne risquons-nous pas, de fait, de restreindre les possibilités actuellement utilisées par les services de la DGSI ?

Cela dit, si nous ne conservions que la première partie de l'article 1er, le groupe UMP n'aurait plus à défendre dans l'hémicycle qu'une proposition de loi se résumant à quelques lignes. Ce ne serait guère respectueux des droits de l'opposition. Mieux vaut, je crois, voter contre tous les articles, ce qui permettra d'inscrire le texte complet à l'ordre du jour de la séance publique et d'en débattre avec les parlementaires qui ne siègent pas à la commission des Lois. Si la majorité ne vote aujourd'hui que ce qu'elle approuve, l'espace de discussion s'en trouvera singulièrement restreint.

*La Commission **rejette** successivement les amendements CL1 et CL5.*

*Elle **rejette** ensuite l'amendement de précision CL7 du rapporteur.*

*Suivant l'avis défavorable du rapporteur, elle **rejette** l'amendement CL6 de M. Sergio Coronado.*

*Elle **rejette** également l'amendement rédactionnel CL8 du rapporteur.*

Elle en vient à l'amendement CL9 du même auteur.

M. le rapporteur. Il s'agit d'élargir doublement le champ des sites internet qui pourraient faire l'objet d'un blocage par les fournisseurs d'accès, à la demande du ministère de l'Intérieur. Seraient visés non seulement les sites faisant l'apologie du terrorisme, mais aussi ceux qui comportent des provocations à des actes de terrorisme. D'autre part, tout contenu sur internet, y compris des messages écrits ou sonores, serait susceptible de justifier un blocage, et pas seulement des images ou des représentations. Cet amendement a la pleine approbation du juge Trévidic.

*La Commission **rejette** l'amendement.*

*Elle **rejette** ensuite l'amendement de conséquence CL10 du même auteur.*

*Elle **rejette** enfin l'article 1er.*

Article 2

(art. 421-2-4-1 [nouveau] du code pénal)

Création d'un délit de consultation de sites internet faisant l'apologie du terrorisme

Cet article vise à créer un nouveau délit, réprimant la consultation habituelle de sites internet provoquant à des actes de terrorisme ou faisant l'apologie du terrorisme.

Un nouvel article 421-2-4-1 serait introduit en ce sens dans le chapitre Ier, intitulé « Des actes de terrorisme », du titre II du livre IV du code pénal. Ce chapitre regroupe l'ensemble des actes de terrorisme réprimés par le code pénal, qui sont de deux ordres :

– des infractions de droit commun commises en lien avec une entreprise à caractère terroriste, c'est-à-dire commises « *intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur* » (article 421-1 du code pénal). Y figurent notamment les atteintes volontaires à la vie ou à l'intégrité des personnes, les enlèvements et séquestrations, les détournements de moyens de transport, les vols, extorsions, destructions, dégradations et détériorations, les infractions en matière informatique, les infractions en matière de groupes de combat et de mouvements dissous, les infractions liées aux armes, produits explosifs ou matières nucléaires, le blanchiment et le délit d'initié ;

– des infractions spécifiques, telles que le terrorisme écologique (article 421-2), l'association de malfaiteurs en relation avec une entreprise terroriste (article 421-2-1), le financement du terrorisme (article 421-2-2), la non-justification de ressources en cas de relations habituelles avec des personnes se livrant à des actes de terrorisme (article 421-2-3) ou, depuis la loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme, le recrutement terroriste (article 421-2-4).

1. La définition du nouveau délit

Aux termes du présent article, la nouvelle incrimination réprimerait « *le fait de consulter de façon habituelle un service de communication au public en ligne mettant à disposition des messages, soit provoquant directement à des actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ces messages comportent des images montrant la commission d'actes de terrorisme consistant en des atteintes volontaires à la vie* » (nouvel article 421-2-4-1 du code pénal).

Ces dispositions s'inscriraient dans l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public, mais aussi, dans le cas où l'internaute concerné serait déjà « passé à l'acte », dans celui de recherche des auteurs d'infractions. Rappelons que, pour le Conseil constitutionnel, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions sont « *toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle* » [(1)].

La répression d'une consultation habituelle sur internet **s'inspire en partie de l'article 227-23 du code pénal, issu de la loi n° 2007-293 du 5 mars 2007 réformant la protection de l'enfance, qui sanctionne la consultation de sites pédopornographiques** [(2)]. Cet article punit de deux ans d'emprisonnement et de 30 000 euros le fait de consulter habituellement – ou, depuis 2013 [(3)], en contrepartie d'un paiement – un service de communication au public en ligne mettant à disposition l'image ou la représentation d'un mineur présentant un caractère pornographique. Il permet de condamner les individus qui, auparavant, échappaient à la répression parce qu'ils n'avaient ni imprimé ni enregistré sur un support (un disque dur par exemple) les images à caractère pornographique de mineurs consultées sur un site internet [(4)].

---

(1) Décision n° 2004-492 DC du 2 mars 2004, Loi portant adaptation de la justice aux évolutions de la criminalité.

(2) Depuis, la directive 2011/92/UE du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie impose aux États membres de l'Union européenne de punir d'une peine privative de liberté le fait « d'accéder, en connaissance de cause et par le biais des technologies de l'information et de la communication, à de la pédopornographie *».*

(3) Article 5 de la loi n° 2013-711 du 5 août 2013 portant diverses dispositions d'adaptation dans le domaine de la justice en application du droit de l'Union européenne et des engagements internationaux de la France.

(4) Cour de cassation, crim., 5 janvier 2005, n° 04-82.524.

On relèvera que, si la loi du 5 mars 2007 précitée n'a pas été soumise au contrôle du Conseil constitutionnel, la Cour de cassation a, le 6 juin 2012, rejeté une question prioritaire de constitutionnalité (QPC) dirigé contre l'article 227-23, faute de moyen sérieux [(1)].

Afin de satisfaire le principe de légalité des délits et des peines et de respecter la liberté de communication, **la rédaction proposée au présent article vise des faits bien précis, la constitution du délit supposant ainsi la réunion de plusieurs éléments**.

En premier lieu, il s'agit de **consulter « *un service de communication au public en ligne* »**, autrement dit un site internet – ce qui inclut notamment les réseaux sociaux. Votre rapporteur renvoie sur ce point aux développements précédents, relatifs à la faculté de blocage des sites faisant l'apologie du terrorisme [(2)].

En deuxième lieu, la consultation doit être effectuée **« *de façon habituelle* »**. Plusieurs connexions sont donc nécessaires, durant un laps de temps plus ou moins long. À titre indicatif, en matière de pédopornographie, la consultation de plusieurs sites en l'espace de 48 heures a déjà été considérée comme « habituelle » au sens de l'article 227-23 du code pénal [(3)].

En troisième lieu, cette consultation doit concerner des **sites « *mettant à disposition des messages* » :**

– soit **provoquant directement à des actes de terrorisme** ;

– soit **faisant l'apologie de ces actes lorsque, à cette fin, ces messages comportent des images montrant la commission d'actes de terrorisme consistant en des atteintes volontaires à la vie**.

La distinction entre ces deux catégories de sites reprend les termes du délit prévu au sixième alinéa de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse, qui punit de cinq ans d'emprisonnement et de 45 000 euros d'amende ceux qui, par voie de presse ou par tout autre moyen de publication [(4)], « *auront provoqué directement aux actes de terrorisme prévus par le titre II du livre IV du code pénal, ou qui en auront fait l'apologie* ».

---

(1) Cour de cassation, crim., 6 juin 2012, n° 12-90.016.

(2) Voir supra *le commentaire de l'article 1er, point 2 b.*

(3) Cour administrative d'appel de Nantes, 20 octobre 2011, n° 10NT00535.

(4) Ces moyens sont définis à l'article 23 de la même loi : il s'agit « des discours, cris ou menaces proférés dans des lieux ou réunions publics, (…) des écrits, imprimés, dessins, gravures, peintures, emblèmes, images ou tout autre support de l'écrit, de la parole ou de l'image vendus ou distribués, mis en vente ou exposés dans des lieux ou réunions publics, (…) des placards ou des affiches exposés au regard du public, [et de] tout moyen de communication au public par voie électronique ». *L'ajout de* « tout moyen de communication au public par voie électronique » *résulte de la loi n° 2004-575 du 21 juin 2004 précitée.*

Dans le premier cas – celui de la *provocation directe* à des actes de terrorisme –, peu importe la forme que prennent les messages en question : il peut s'agir d'écrits comme de photos ou de vidéos.

Dans le second cas – celui de l'*apologie* du terrorisme –, il est nécessaire, pour que le délit prévu au présent article soit constitué, que les messages en question **comportent des « *images montrant la commission d'actes de terrorisme consistant en des atteintes volontaires à la vie* »** (1). L'exigence est donc double. D'une part, un site internet constitué d'une série de textes faisant l'apologie du terrorisme, mais dépourvu de toute image (photo, vidéos, etc.), ne tomberait pas sous le coup du nouveau délit. En décider autrement rendrait plus difficile la caractérisation de l'infraction. D'autre part, les images présentes sur le site ne doivent pas montrer n'importe quels actes de terrorisme, mais des « *atteintes volontaires à la vie* », formulation reprise du 1° de l'article 421-1 du code pénal précité. Là encore, cette exigence procède de la volonté de ne faire porter la nouvelle incrimination que sur les sites les plus ouvertement choquants, sur lesquels l'internaute ne saurait avoir le moindre doute quant à l'illégalité des images consultées. **Concrètement, il s'agirait par exemple de certains sites montrant des décapitations ou des exécutions**, comme l'avait suggéré, en 2012, Mme Nathalie Kosciusco-Morizet (2).

Le champ d'application du présent article est donc plus restreint que celui de l'article 1er, qui ouvre la possibilité de bloquer l'accès à des sites internet, dès lors que ceux-ci diffusent des images ou des représentations faisant l'apologie de *n'importe quel* acte terrorisme – pas seulement les atteintes volontaires à la vie – prévu par le titre II du livre IV du code pénal (articles 421-1 à 421-6).

Par construction, le présent article ne trouverait à s'appliquer qu'aux sites internet ne figurant pas sur la « liste noire » des sites concernés par le blocage prévu à l'article 1er. Les services du ministère de l'Intérieur auront ainsi toute latitude pour laisser libre l'accès à certains sites, sur lesquels pourrait être constatée la commission du nouveau délit de consultation habituelle, le cas échéant repérée grâce aux « cyberpatrouilles » prévues à l'article 4 de la présente proposition de loi. Contrairement à certaines craintes exprimées devant votre commission des Lois (3), il n'existe donc aucune contradiction entre ces différentes mesures, qui se caractérisent au contraire par leur complémentarité.

2. La répression du nouveau délit

Le dernier alinéa du présent article prévoit **que le nouveau délit ne serait pas applicable « *lorsque la consultation résulte de l'exercice normal d'une profession ayant pour objet d'informer le public, intervient dans le cadre de***

---

(1) C'est la conséquence des termes : « à cette fin *» prévus au présent article.*

(2) Voir les débats en commission des Lois le 14 novembre 2012 (compte-rendu n° 12), ainsi que le point de vue : « Le terrorisme doit être aussi pourchassé sur internet », Le Monde, *7 novembre 2012.*

(3) Voir l'intervention de Mme Marie-Françoise Bechtel le 30 avril 2014 (compte-rendu n° 52).

recherches scientifiques ou est réalisée afin de servir de preuve en justice **»**. Il s'agit de ménager la possibilité de consulter des sites faisant l'apologie du terrorisme lorsque cette consultation est animée par des motifs légitimes.

Seraient ainsi concernés les journalistes et les chercheurs, à condition que la consultation procède de l'exercice normal de leur profession. Dans le cas des journalistes, il s'agirait par exemple de respecter la loi de 1881 précitée, en particulier son article 35 *quater*, qui interdit la diffusion de la reproduction des circonstances d'un crime ou d'un délit qui porterait gravement atteinte à la dignité d'une victime. De la même façon, un universitaire agissant dans le cadre de recherches sur les phénomènes terroristes pourrait consulter les sites internet visés par le présent article. La nécessité de fournir une preuve en justice fournirait un autre motif légitime de consultation.

Ces cas d'exonération de l'infraction sont proches de ceux déjà prévus par le code pénal, à propos du délit dit de « *happy slapping* » – ou « vidéoagression » –, consistant à filmer, en vue de sa diffusion, l'agression physique d'une personne, généralement à l'aide d'un téléphone portable ou d'un smartphone. Issu de la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance, l'article 222-33-3 du code pénal punit ainsi l'enregistrement et la diffusion d'images montrant des atteintes volontaires à l'intégrité d'une personne. Ces dispositions ne sont, toutefois, pas applicables « *lorsque l'enregistrement ou la diffusion résulte de l'exercice normal d'une profession ayant pour objet d'informer le public ou est réalisé afin de servir de preuve en justice* ».

Le nouveau délit de consultation habituelle de sites faisant l'apologie du terrorisme serait **puni de deux ans d'emprisonnement et de 30 000 euros d'amende**, soit les mêmes peines qu'en matière de consultation habituelle de sites pédopornographiques.

Comme pour toutes les infractions en matière de terrorisme, des **peines complémentaires** seraient applicables :

– interdictions des droits civiques, civils et de famille, interdictions professionnelles et interdiction de séjour, prévues à l'article 422-3 du code pénal ;

– interdiction de territoire prévu à l'article 422-4 du même code ;

– confiscation de biens prévue à l'article 422-6 du même code.

À l'instar du délit de consultation de sites pédopornographiques, **l'acte de consultation pourrait être établi de plusieurs manières** :

– en analysant l'historique de navigation d'un internaute dont l'ordinateur aurait été saisi lors d'une enquête ou aurait fait l'objet d'une perquisition à distance. Rappelons, en effet, que, **depuis la LOPPSI 2, l'article 706-102-1 du**

code de procédure pénale permet la captation de données informatiques [(1)]. Entendu par votre rapporteur, le juge d'instruction Marc Trévidic a néanmoins regretté que ces mesures ne soient toujours pas entrées en application, faute de désignation des agents spécialisés pouvant procéder à ces captations. En tout état de cause, la constatation de l'infraction suppose que l'individu concerné ait déjà été repéré ;

– en se procurant, auprès des fournisseurs d'accès à internet ou des hébergeurs, les données de connexion des internautes concernés, comme le permet la législation actuelle en vue de « *prévenir les actes de terrorisme* » [(2)], législation récemment renforcée par la dernière loi de programmation militaire [(3)]. Cela suppose toutefois que ces prestataires techniques aient conservé les données en question [(4)]. Là encore, le précédent de la lutte contre la pédopornographie peut servir d'exemple, dans la mesure où « *en pratique, des réquisitions sont couramment adressées aux opérateurs par les officiers de police judiciaire sous le contrôle du procureur de la République ou du juge d'instruction afin d'identifier les auteurs d'infractions en matière de pédopornographie commises au moyen d'internet. Il s'agit, en effet, du moyen le plus efficace d'identifier les auteurs de ces agissements* via *notamment l'obtention de l'adresse IP et de l'identification de son propriétaire* » [(5)] ;

– grâce aux contacts noués et aux éléments de preuve rassemblés par des « cyberpatrouilleurs » spécialement formés à cet effet, ainsi que le permettrait l'article 4 de la présente proposition de loi.

---

(1) « Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction. »

(2) Article L. 34-1-1 du code des postes et des communications électroniques et II bis *de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée. Ces articles prévoient que des agents des services de police et de gendarmerie spécialement habilités peuvent «* exiger *», auprès des fournisseurs d'accès et des hébergeurs, la communication des données de connexion d'internautes.*

(3) En application de l'article 20 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, les dispositions citées dans la note précédente seront, à compter du 1er janvier 2015, remplacées par les articles L. 246-1 et suivants du code de la sécurité intérieure.

(4) L'obligation de conservation des données ne concerne que celles « de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus *» du site concerné (II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée). La nature des données en question est précisée dans le décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.*

(5) Étude d'impact du projet de loi renforçant la prévention et la répression du terrorisme, déposé à l'Assemblée nationale le 11 avril 2012, n° 4497.

*

* *

Après avis défavorable du rapporteur, la Commission ***rejette*** *l'amendement de suppression CL2 de M. Sergio Coronado.*

Elle ***rejette*** *successivement les amendements rédactionnels CL11 et CL17 du rapporteur.*

Puis elle ***rejette*** *l'article 2.*

Après l'article 2

La Commission est saisie de l'amendement CL12 du rapporteur.

M. le rapporteur. La majorité n'est pas favorable, je l'ai bien compris, à la création du délit de consultation habituelle des sites faisant l'apologie du terrorisme. Mais, dans l'hypothèse où elle l'aurait été, elle aurait d'autant plus approuvé cet amendement qui concerne les mineurs âgés de treize à seize ans, non pas pour les punir d'une peine de prison, mais pour leur faire accomplir un stage de prévention spécialement adapté. Cette idée nous a été suggérée par l'Association française des victimes du terrorisme, présidée par M. Guillaume Denoix de Saint Marc. Elle prospère également au sein du CRIF et dans les milieux associatifs qui, à Bruxelles, s'intéressent à ces questions. Tout un travail est à faire pour éduquer ou désendoctriner les mineurs les plus jeunes. C'est ce que les experts appellent le « discours contre-narratif ».

Mme Marie-Françoise Bechtel. L'audition des représentants des victimes était en effet extrêmement intéressante. La réflexion a tout de même bien avancé depuis l'époque où Mme Nathalie Kosciusko-Morizet soutenait un amendement beaucoup plus répressif ! Nous lui avions objecté à l'époque que, lorsque les enfants se font endoctriner dans les cours de récréation ou s'échangent des vidéos violentes, le principal sujet était la protection de l'enfance. J'avais d'ailleurs suggéré une recherche en ce sens.

Cela dit, si l'amendement est intéressant, il ne me semble pas de très bonne pratique législative qu'une modification de l'ordonnance de 1945 relative à l'enfance délinquante figure dans une loi de lutte contre l'apologie du terrorisme.

M. le rapporteur. Si c'est là le seul problème, je suis tout disposé à modifier mon amendement pour que la disposition ne soit pas insérée dans l'ordonnance de 1945.

La Commission ***rejette*** *l'amendement.*

Article 3

(art. 706-25-1, 706-88 et 706-94-1 [nouveau] du code de procédure pénale)

Procédure pénale applicable à la consultation de sites internet faisant l'apologie du terrorisme

Cet article vise à définir les règles de procédure pénale applicables au délit, créé à l'article 2, de consultation de sites internet faisant l'apologie du terrorisme.

Du fait même de son insertion dans le chapitre I^er^, intitulé « *Des actes de terrorisme* », du titre II du livre IV du code pénal, le délit prévu au nouvel article 421-2-4-1, donnerait lieu à l'application des règles de procédure pénale spécifiques à la répression du terrorisme et exorbitantes du droit commun (régime particulier de garde à vue, de prescription de l'action publique, de perquisitions etc.).

Or, pour justifier l'application de règles de procédure spécifiques, la jurisprudence du Conseil constitutionnel exige que les infractions concernées revêtent « *une gravité et une complexité particulières* » (1). Dans le cas contraire, ces procédures spéciales « *imposeraient une rigueur non nécessaire* », au sens de l'article 9 de la Déclaration des droits de l'homme de 1789, selon lequel « *[tout] homme étant présumé innocent jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être sévèrement réprimée par la loi* » (2).

En conséquence, afin de veiller à la proportionnalité entre la gravité des faits couverts par la nouvelle infraction et la procédure pénale qui lui serait applicable, **le présent article tend à exclure plusieurs des règles propres au terrorisme, rapprochant ainsi le nouveau délit de la procédure pénale de droit commun**.

C'est ainsi que :

– **le délai de prescription applicable au nouveau délit de consultation serait le délai de droit commun de trois ans**, prévu à l'article 8 du code de procédure pénale, et non pas le délai de vingt ans prévu, pour les délits en matière de terrorisme, au dernier alinéa de l'article 706-25-1 du même code (3) (**1°** du présent article) ;

---

(1) Voir, par exemple, la décision n° 2004-492 DC du 2 mars 2004, Loi portant adaptation de la justice aux évolutions de la criminalité.

(2) Voir, par exemple, la décision n° 2010-31 QPC du 22 septembre 2010, M. Bulent A. et autres [Garde à vue terrorisme].

(3) L'article 706-16 du code de procédure pénale soumet « les actes de terrorismes incriminés par les articles 421-1 à 421-6 du code pénal *» aux dispositions du titre XV, intitulé «* De la poursuite, de l'instruction et du jugement des actes de terrorisme *», du livre IV du code de procédure pénale, lequel comprend notamment l'article 706-25-1 précité, relatif aux délais de prescription.*

– **le régime de garde à vue applicable serait celui de droit commun**, et non pas celui prévu à l'article 706-88 du code de procédure pénale [(1)] (**2°** du présent article). La durée maximale de garde à vue serait donc de 48 heures, et non pas de 96 heures comme en matière de terrorisme. Les possibilités, spécifiques au terrorisme, de report de l'intervention de l'avocat ne seraient pas non applicables ;

– **les perquisitions de nuit seraient interdites** (**3°** du présent article). Un nouvel article 706-94-1 du code de procédure pénale exclurait expressément l'application des dispositions de la section IV du chapitre II du titre XXV du livre IV du même code (articles 706-89 à 706-94) [(2)], qui autorisent les perquisitions hors des heures habituelles (de 6 h à 21 h).

En revanche, les *autres* règles de procédure spécifiques à la répression du terrorisme seraient applicables au nouveau délit de consultation habituelle de sites faisant l'apologie du terrorisme, en particulier la centralisation des affaires à Paris et les règles régissant la surveillance des personnes, les infiltrations, les interceptions de correspondances, les sonorisations et fixations d'images et la captation de données informatiques [(3)].

*
* *

Suivant l'avis défavorable du rapporteur, la Commission ***rejette*** *l'amendement CL3 de M. Sergio Coronado.*

Elle ***rejette*** *ensuite l'amendement rédactionnel et de conséquence CL13 et l'amendement de précision CL14 du rapporteur.*

Elle ***rejette*** *enfin l'article 3.*

Article 4
(art. 706-25-2 du code de procédure pénale)
Cyberpatrouilles sur les sites internet faisant l'apologie du terrorisme

Cet article vise à étendre les capacités d'investigation de la police en matière d'infractions à la législation anti-terroriste commises par un moyen de communication électronique. Il s'agit d'**élargir les moyens des « cyberpatrouilleurs »**, aujourd'hui chargés de constater les délits de provocation au terrorisme ou d'apologie du terrorisme.

---

(1) Lequel est applicable aux infractions entrant dans le champ d'application de l'article 706-73 du code de procédure pénale, dont le 11° vise les infractions de terrorisme prévues aux articles 421-1 à 421-6 du code pénale.

(2) Ces articles sont applicables aux infractions entrant dans le champ d'application de l'article 706-73 du code de procédure pénale, dont le 11° vise les infractions de terrorisme prévues aux articles 421-1 à 421-6 du code pénale.

(3) Respectivement : articles 706-17, 706-80, 706-81, 706-95, 706-96 et 706-102-1 du code de procédure pénale.

1. Une technique d'investigation éprouvée

La « cyberpatrouille » – dite également « cyberinfiltration » – est une technique d'investigation consistant à **autoriser des enquêteurs, affectés dans un service spécialisé et expressément habilités, à procéder à certains actes sans être pénalement responsables, et ce sans toutefois pouvoir inciter à la commission des infractions** qu'ils sont chargés de constater.

Les actes en question consistent à :

– participer sous un **pseudonyme** aux échanges électroniques ;

– être **en contact** par un moyen de communication électronique avec les personnes susceptibles d'être les auteurs d'infraction ;

– extraire, acquérir ou conserver des éléments de **preuve** et des **données** relatives aux personnes soupçonnées d'infraction.

L'infiltration apparaît d'autant plus utile que, comme on l'a vu, les obligations de conservation des données pesant sur les fournisseurs d'accès à internet et sur les hébergeurs de sites portent sur les seules *données d'identification* des internautes (adresse IP, identifiant, date et heure de connexion, etc.), et non pas sur les *contenus* produits ou échangés par eux [(1)].

Cette méthode d'investigation a été introduite pour la première fois dans notre droit pénal par la **loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance**. En application des articles 706-35-1 et 706-47-3 du code de procédure pénale, elle est aujourd'hui applicable à la constatation des infractions suivantes :

– la traite des êtres humains (articles 225-4-1 à 225-4-9 du code pénal) ;

– le proxénétisme (articles 225-5 à 225-12 du code pénal) ;

– la prostitution de mineurs ou de personnes vulnérables (articles 225-12-1 à 225-12-4 du code pénal) ;

– certaines infractions de mise en péril de mineurs : pédopornographie, provocation à l'usage illicite de stupéfiants, à la consommation d'alcool, à la commission de crimes ou délits (articles 227-18 à 227-24 du code pénal).

La technique de « cyberpatrouille » a, ensuite, été étendue à la constatation des infractions commises à l'occasion de paris ou de jeux d'argent ou de hasard en ligne, en application de la **loi n° 2010-476 du 12 mai 2010 relative à l'ouverture**

(1) Voir en ce sens le II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 précitée. Voir également supra *le commentaire de l'article 1er de la présente proposition de loi.*

à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne [(1)].

Plus récemment, l'**ordonnance n° 2013-1183 du 19 décembre 2013 relative à l'harmonisation des sanctions pénales et financières relatives aux produits de santé et à l'adaptation des prérogatives des autorités et des agents chargés de constater les manquements** a introduit un dispositif similaire pour réprimer une série d'infractions en matière sanitaire (article 706-2-2 du code de procédure pénale) [(2)]. Sont notamment concernées les infractions relatives aux produits de santé, par exemple la vente de faux médicaments sur internet.

2. Les cyberpatrouilles en matière de terrorisme

L'article 34 de la **loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2)** a prévu le même dispositif de « cyberpatrouilles » en matière d'infractions, commises par un moyen de communication électronique, **de provocation au terrorisme et d'apologie du terrorisme**, prévues au sixième alinéa de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse.

En application de l'article 706-25-2 du code de procédure pénale, les policiers compétents sont chargés **de constater ces infractions, d'en rassembler les preuves et d'en rechercher les auteurs**, au moyen des méthodes précitées : « *dans le but de constater les infractions mentionnées au sixième alinéa de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé désigné par arrêté du ministre de l'Intérieur et spécialement habilités à cette fin, procéder aux actes suivants sans en être pénalement responsables :*

« 1° Participer sous un pseudonyme aux échanges électroniques ;

« 2° Être en contact par ce moyen avec les personnes susceptibles d'être les auteurs de ces infractions ;

« 3° Extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions.

« À peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions. »

---

(1) Ces dispositions ont été renforcées par l'article 21 de la loi de finances rectificative pour 2012 (n° 2012-354 du 14 mars 2012).

(2) Infractions prévues aux articles L. 5421-2, L. 5421-3, L. 5421-13, L. 5426-1, L. 5432-1, L. 5432-2, L. 5438-4, L. 5439-1, L. 5451-1, L. 5461-3 et L. 5462-3 du code de la santé publique, ainsi qu'à l'article L. 213-1 du code de la consommation.

Ces dispositions n'ont toutefois été mises en œuvre que depuis peu :

– **un arrêté ministériel du 19 septembre 2011** fixe la liste des services ou unités autorisés à mettre en œuvre des investigations sous pseudonyme. Il s'agit notamment de la sous-direction antiterroriste de la direction centrale de la police judiciaire (DCPJ), de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) et de la direction générale de la sécurité intérieure (DGSI) [(1)] ;

– **un arrêté ministériel du 24 juin 2013** dispose que les officiers et agents doivent avoir été « *spécialement habilités par le procureur général près la cour d'appel de Paris* », après agrément du service auquel ils sont attachés. Ils doivent au préalable avoir reçu une « *formation spécifique* » ;

– **une circulaire du 10 septembre 2013** de la directrice des affaires criminelles et des grâces [(2)] précise que les services ou unités compétents peuvent recourir aux « cyberpatrouilles » de leur propre initiative, ou bien au profit des autres services et unités de police judiciaire ou encore sur saisine d'un magistrat, en vue d'appuyer une enquête en cours. Les pseudonymes utilisés par les « cyberpatrouilleurs » sont préalablement déclarés au service interministériel d'assistance technique (SIAT) de la DCPJ, qui en assure la centralisation et renseigne dans les plus brefs délais les « cyberpatrouilleurs » sur la disponibilité ou non de tout pseudonyme nouvellement choisi. En cas d'urgence, le pseudonyme peut être utilisé sans attendre la validation, qui est alors délivrée *a posteriori*.

Le présent article tend à **élargir le champ de l'article 706-25-2 du code de procédure pénale, afin d'y inclure le délit, créé à l'article 2 de la présente proposition, de consultation habituelle de sites internet faisant l'apologie du terrorisme**. Des « cyberpatrouilleurs » pourront ainsi être chargés de repérer des internautes tombant sous le coup du nouveau délit et, partant, de rassembler les preuves à même de les faire condamner.

*

* *

Suivant l'avis défavorable du rapporteur, la Commission ***rejette*** *l'amendement CL4 de M. Sergio Coronado.*

Elle ***rejette*** *ensuite l'amendement rédactionnel et de conséquence CL15 du rapporteur.*

Elle ***rejette*** *enfin l'article 4.*

---

(1) Cette dernière a succédé à la direction centrale du renseignement intérieur (DCRI) en application du décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure.

(2) Circulaire du 10 septembre 2013 relative aux investigations sous pseudonyme par voie d'échanges électroniques en matière de provocation et d'apologie des actes de terrorisme.

Après l'article 4

La Commission ***rejette*** *l'amendement CL16 du rapporteur, visant à instaurer un régime juridique permettant les investigations sous pseudonyme par voie d'échanges électroniques.*

Tous les articles ayant été rejetés, il n'y a pas lieu pour la Commission de se prononcer sur l'ensemble de la proposition de loi, qui est ainsi ***rejetée.***

*

* *

En conséquence, la commission des Lois constitutionnelles, de la législation et de l'administration générale de la République vous demande de ***rejeter*** *la proposition de loi renforçant la lutte contre l'apologie du terrorisme sur internet (n° 1907).*

TABLEAU COMPARATIF

___

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par la Commission
___	___	___
	Proposition de loi renforçant la lutte contre l'apologie du terrorisme sur internet	**Proposition de loi renforçant la lutte contre l'apologie du terrorisme sur internet**
Loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique	Article 1er	Article 1er
Art. 6. – I. – 1. – 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. Les personnes visées à l'alinéa précédent les informent également de l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle et leur proposent au moins un des moyens figurant sur la liste prévue au deuxième alinéa de l'article L. 331-26 du même code. 2. Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès	*Le 7° du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est ainsi modifié :*	**Supprimé**

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par la Commission
impossible. L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa. 3. Les personnes visées au 2 ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible. L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa. 4. Le fait, pour toute personne, de présenter aux personnes mentionnées au 2 un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'une peine d'un an d'emprisonnement et de 15 000 € d'amende. 5. La connaissance des faits litigieux est présumée acquise par les personnes désignées au 2 lorsqu'il leur est notifié les éléments suivants : – la date de la notification ; – si le notifiant est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ; si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ; – les nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ;		

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par la Commission
– la description des faits litigieux et leur localisation précise ;		
– les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;		
– la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.		
6. Les personnes mentionnées aux 1 et 2 ne sont pas des producteurs au sens de l'article 93-3 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle.		
7. Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites.		
Le précédent alinéa est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire.		
Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie enfantine, de l'incitation à la violence, notamment l'incitation aux violences faites aux femmes, ainsi que des atteintes à la dignité humaine, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et aux articles 227-23 et 227-24 du code pénal.	*1° Au troisième alinéa, après le mot : « humanité », sont insérés les mots : « , des crimes visés par les articles 421-1 à 421-2-2 du code pénal, » ;*	
	2° Il est complété par deux alinéas ainsi rédigés :	
	« Lorsque les nécessités de la lutte contre la diffusion d'images ou de	

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par la Commission
	représentations faisant l'apologie des actes de terrorisme prévus par le titre II du livre IV du code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 du présent I les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai.	
	« Un décret en Conseil d'État fixe les modalités d'application de l'alinéa précédent. »	
À ce titre, elles doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites.		
Lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 du présent I les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai.		
Un décret fixe les modalités d'application de l'alinéa précédent, notamment celles selon lesquelles sont compensés, s'il y a lieu, les surcoûts résultant des obligations mises à la charge des opérateurs.		
Compte tenu de l'intérêt général attaché à la répression des activités illégales de jeux d'argent, les personnes mentionnées aux 1 et 2 mettent en place, dans des conditions fixées par décret, un dispositif facilement accessible et visible permettant de signaler à leurs		

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par la Commission
abonnés les services de communication au public en ligne tenus pour répréhensibles par les autorités publiques compétentes en la matière. Elles informent également leurs abonnés des risques encourus par eux du fait d'actes de jeux réalisés en violation de la loi. Tout manquement aux obligations définies aux quatrième, cinquième et septième alinéas est puni des peines prévues au 1 du VI. . . . . . . VI.-1. Est puni d'un an d'emprisonnement et de 75 000 Euros d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux 1 et 2 du I, de ne pas satisfaire aux obligations définies aux quatrième, cinquième et septième alinéas du 7 du I, de ne pas avoir conservé les éléments d'information visés au II ou de ne pas déférer à la demande d'une autorité judiciaire d'obtenir communication desdits éléments. . . . . . . **Code pénal** *Art. 421-1 à 421-2-2. – Cf. annexe*	Article 2 *Après l'article 421-2-4 du code pénal, il est inséré un article 421-2-4-1 ainsi rédigé :* *« Art. 421-2-4-1. – Est puni de deux ans d'emprisonnement et 30 000 euros d'amende le fait de consulter de façon habituelle un service de communication au public en ligne mettant à disposition des messages, soit provoquant directement à des actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ces messages comportent des images montrant la commission d'actes de terrorisme consistant en des atteintes volontaires à*	Article 2 **Supprimé**

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par la Commission
___	___	___
	la vie. *« Le présent article n'est pas applicable lorsque la consultation résulte de l'exercice normal d'une profession ayant pour objet d'informer le public, intervient dans le cadre de recherches scientifiques ou est réalisée afin de servir de preuve en justice. »*	
	Article 3	Article 3
Code de procédure pénale	*Le code de procédure pénale est ainsi modifié :*	**Supprimé**
Art. 706-25-1. – L'action publique des crimes mentionnés à l'article 706-16 se prescrit par trente ans. La peine prononcée en cas de condamnation pour l'un de ces crimes se prescrit par trente ans à compter de la date à laquelle la condamnation est devenue définitive. L'action publique relative aux délits mentionnés à l'article 706-16 se prescrit par vingt ans. La peine prononcée en cas de condamnation pour ces délits se prescrit par vingt ans à compter de la date à laquelle la condamnation est devenue définitive.	*1° L'article 706-25-1 est complété par un alinéa ainsi rédigé :* *« Les dispositions du présent article ne sont toutefois pas applicables au délit prévu par l'article 421-2-4 du code pénal. » ;*	
Art. 706-88. – Pour l'application des articles 63, 77 et 154, si les nécessités de l'enquête ou de l'instruction relatives à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent, la garde à vue d'une personne peut, à titre exceptionnel, faire l'objet de deux prolongations supplémentaires de vingt-quatre heures chacune. Ces prolongations sont autorisées, par décision écrite et motivée, soit, à la requête du procureur de la République, par le juge des libertés et de la détention, soit par le juge d'instruction	*2° L'article 706-88 est complété par un alinéa ainsi rédigé :*	

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par la Commission
La personne gardée à vue doit être présentée au magistrat qui statue sur la prolongation préalablement à cette décision. La seconde prolongation peut toutefois, à titre exceptionnel, être autorisée sans présentation préalable de la personne en raison des nécessités des investigations en cours ou à effectuer. Lorsque la première prolongation est décidée, la personne gardée à vue est examinée par un médecin désigné par le procureur de la République, le juge d'instruction ou l'officier de police judiciaire. Le médecin délivre un certificat médical par lequel il doit notamment se prononcer sur l'aptitude au maintien en garde à vue, qui est versé au dossier. La personne est avisée par l'officier de police judiciaire du droit de demander un nouvel examen médical. Ces examens médicaux sont de droit. Mention de cet avis est portée au procès-verbal et émargée par la personne intéressée ; en cas de refus d'émargement, il en est fait mention. Par dérogation aux dispositions du premier alinéa, si la durée prévisible des investigations restant à réaliser à l'issue des premières quarante-huit heures de garde à vue le justifie, le juge des libertés et de la détention ou le juge d'instruction peuvent décider, selon les modalités prévues au deuxième alinéa, que la garde à vue fera l'objet d'une seule prolongation supplémentaire de quarante-huit heures. Par dérogation aux dispositions des articles 63-4 à 63-4-2, lorsque la personne est gardée à vue pour une infraction entrant dans le champ d'application de l'article 706-73, l'intervention de l'avocat peut être différée, en considération de raisons impérieuses tenant aux circonstances particulières de l'enquête ou de l'instruction, soit pour permettre le recueil ou la conservation des preuves, soit pour prévenir une atteinte aux personnes, pendant une durée maximale de quarante-huit heures ou, s'il s'agit d'une infraction mentionnée aux 3° ou 11° du même article 706-73, pendant une durée maximale de soixante-douze		

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par la Commission
heures. Le report de l'intervention de l'avocat jusqu'à la fin de la vingt-quatrième heure est décidé par le procureur de la République, d'office ou à la demande de l'officier de police judiciaire. Le report de l'intervention de l'avocat au-delà de la vingt-quatrième heure est décidé, dans les limites fixées au sixième alinéa, par le juge des libertés et de la détention statuant à la requête du procureur de la République. Lorsque la garde à vue intervient au cours d'une commission rogatoire, le report est décidé par le juge d'instruction. Dans tous les cas, la décision du magistrat, écrite et motivée, précise la durée pour laquelle l'intervention de l'avocat est différée Lorsqu'il est fait application des sixième et septième alinéas du présent article, l'avocat dispose, à partir du moment où il est autorisé à intervenir en garde à vue, des droits prévus aux articles 63-4 et 63-4-1, au premier alinéa de l'article 63-4-2 et à l'article 63-4-3.	*« Les dispositions du présent article ne sont pas applicables au délit prévu par l'article 421-2-4 du code pénal. » ;* *3° La section 4 du titre XXV du livre IV est complétée par un article 706-94-1 ainsi rédigé :* *« Art. 706-94-1. – Les dispositions de la présente section ne sont pas applicables au délit prévu par l'article 421-2-4 du code pénal. »*	
Code pénal *Art. 421-2-4. – Cf. annexe*		
Code de procédure pénale	Article 4	Article 4
Art. 706-25-2. – Dans le but de constater les infractions mentionnées au sixième alinéa de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et lorsque celles-ci sont commises par un moyen de communication	*Au premier alinéa de l'article 706-25-2, après le mot :*	**Supprimé**

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par la Commission
électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé désigné par arrêté du ministre de l'intérieur et spécialement habilités à cette fin, procéder aux actes suivants sans en être pénalement responsables : 1° Participer sous un pseudonyme aux échanges électroniques ; 2° Etre en contact par ce moyen avec les personnes susceptibles d'être les auteurs de ces infractions ; 3° Extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions. À peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions. **Code pénal** *Art. 421-2-4. – Cf. annexe*	*« électronique, », sont insérés les mots : « , ainsi que l'infraction prévue et réprimée par l'article 421-2-4 du code pénal ».*	

ANNEXE AU TABLEAU COMPARATIF

Code pénal

Art. 421-1. – Constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes :

1° Les atteintes volontaires à la vie, les atteintes volontaires à l'intégrité de la personne, l'enlèvement et la séquestration ainsi que le détournement d'aéronef, de navire ou de tout autre moyen de transport, définis par le livre II du présent code ;

2° Les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique définis par le livre III du présent code ;

3° Les infractions en matière de groupes de combat et de mouvements dissous définies par les articles 431-13 à 431-17 et les infractions définies par les articles 434-6 et 441-2 à 441-5 ;

4° Les infractions en matière d'armes, de produits explosifs ou de matières nucléaires définies par le I de l'article L. 1333-9, les articles L. 1333-11 et L. 1333-13-2, le II des articles L. 1333-13-3 et L. 1333-13-4, les articles L. 1333-13-6, L. 2339-2, L. 2339-14, L. 2339-16, L. 2341-1, L. 2341-4, L. 2341-5, L. 2342-57 à L. 2342-62, L. 2353-4, le 1° de l'article L. 2353-5 et l'article L. 2353-13 du code de la défense, ainsi que les articles L. 317-4, L. 317-7 et L. 317-8 à l'exception des armes de la catégorie D définies par décret en Conseil d'État, du code de la sécurité intérieure ;

5° Le recel du produit de l'une des infractions prévues aux 1° à 4° ci-dessus ;

6° Les infractions de blanchiment prévues au chapitre IV du titre II du livre III du présent code ;

7° Les délits d'initié prévus à l'article L. 465-1 du code monétaire et financier.

Art. 421-2. – Constitue également un acte de terrorisme, lorsqu'il est intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, le fait d'introduire dans l'atmosphère, sur le sol, dans le sous-sol, dans les aliments ou les composants alimentaires ou dans les eaux, y compris celles de la mer territoriale, une substance de nature à mettre en péril la santé de l'homme ou des animaux ou le milieu naturel.

Art. 421-2-1. – Constitue également un acte de terrorisme le fait de participer à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un des actes de terrorisme mentionnés aux articles précédents.

Art. 421-2-2. – Constitue également un acte de terrorisme le fait de financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des

biens quelconques ou en donnant des conseils à cette fin, dans l'intention de voir ces fonds, valeurs ou biens utilisés ou en sachant qu'ils sont destinés à être utilisés, en tout ou partie, en vue de commettre l'un quelconque des actes de terrorisme prévus au présent chapitre, indépendamment de la survenance éventuelle d'un tel acte.

Art. 421-2-4. – Le fait d'adresser à une personne des offres ou des promesses, de lui proposer des dons, présents ou avantages quelconques, de la menacer ou d'exercer sur elle des pressions afin qu'elle participe à un groupement ou une entente prévu à l'article 421-2-1 ou qu'elle commette un des actes de terrorisme mentionnés aux articles 421-1 et 421-2 est puni, même lorsqu'il n'a pas été suivi d'effet, de dix ans d'emprisonnement et de 150 000 € d'amende.

LISTE DES PERSONNES AUDITIONNÉES PAR LE RAPPORTEUR

1. Ministère de l'Intérieur

● Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)

– Mme Valérie Maldonado, commissaire divisionnaire, directrice

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

– M. Thomas Andrieu, maître des requêtes au Conseil d'État, directeur

● Direction générale de la sécurité intérieure (DGSI)

– M. Patrick Calvar, directeur des services actifs de la police nationale, directeur général

– M. François Septours, commissaire, sous-directeur des affaires judiciaires

– M. Dominique Gilles, conseiller juridique

● Unité de coordination de la lutte anti-terroriste (UCLAT)

– M. Loïc Garnier, contrôleur général de la police nationale, chef de l'unité

– M. Antonio Cruz, capitaine de police

2. Pôle anti-terroriste du tribunal de grande instance de Paris

– M. Marc Trévidic, juge d'instruction

3. Représentation permanente de la France auprès de l'Union européenne

– M. Frédéric Veau, préfet, chef du service Justice affaires intérieures (JAI)

4. Conférence des imams de France

– M. Hassen Chalghoumi, président

5. Association Laïcité pour tous

– M. Rezk Shehata, président

6. Conseil représentatif des institutions juives de France (CRIF)

– M. Yonathan Arfi, vice-président

– M. Robert Ejnes, directeur exécutif

7. Association française des victimes du terrorisme (AFVT)

– M. Guillaume Denoix de Saint Marc, directeur général de l'association, membre de la Fédération internationale des associations de victimes du terrorisme

8. Google France

– M. Francis Donnat, maître des requêtes au Conseil d'État en disponibilité, directeur des politiques publiques

– M. Thibault Guiroy, conseiller au service juridique

9. Association des fournisseurs d'accès et de services internet (AFA)

– Mme Carole Gay, responsable des affaires juridiques et réglementaires