Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Avis n°2014-3 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme

Conseil national du numérique
15 Juillet 2014

CNNum
Conseil National du Numérique

Préambule

Le Conseil national du numérique a été saisi le 25 juin 2014 de l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme. Ces dispositions modifient l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) en prévoyant le blocage administratif des sites diffusant des propos ou images provoquant à la commission d'actes terroristes ou en faisant l'apologie. Elles élargissent également le champ des outils de notification imposés aux prestataires techniques.

Afin de rendre un avis le plus éclairé possible dans le court délai imparti, le Conseil a procédé à une quinzaine d'auditions, réunissant des experts du terrorisme (sociologues, journalistes, représentants d'associations), de magistrats et avocats spécialisés, des représentants de la société civile, des membres des services de renseignement et des professionnels du numérique (liste complète disponible en annexe).

Les dispositions soumises à l'appréciation du Conseil s'inscrivent dans un contexte de multiplication des départs de ressortissants français pour la Syrie - le conflit s'y déroulant ayant un effet d'attractivité sans précédent, notamment sur les jeunes.

Le dispositif proposé fait partie du plan gouvernemental visant à renforcer la législation antiterroriste. Il se donne pour objectif de lutter contre le recrutement terroriste en prévoyant la possibilité pour l'autorité administrative de bloquer directement l'accès à certains sites ou contenus.

Cette proposition répond à une situation concrète : un grand nombre de contenus circulant sur internet sous forme de textes, de vidéos, d'images et de sons, met en scène des actes terroristes ou des victimes de conflits pour susciter l'adhésion et l'empathie des internautes. Les plus motivés d'entre eux sont ensuite orientés vers des sites de recrutement, en nombre plus restreint, à partir desquels ils sont repérés pour rejoindre des théâtres d'opérations terroristes. Certains reviennent parfois avec le dessein de commettre des actions en France. Ces deux phases, l'une de diffusion de contenus, l'autre de recrutement, ne peuvent être amalgamées.

Le Conseil national du numérique a déjà eu l'occasion de faire part de son avis sur des sujets connexes[1]. Sans s'opposer au blocage ou au filtrage de contenus quand ils sont illicites, il préconisait en de pareils cas de ne jamais déroger au principe du recours à une autorité judiciaire préalablement à l'instauration d'un dispositif de surveillance, de filtrage ou de blocage de contenus sur Internet. Le dispositif se propose de passer outre ce principe de contrôle judiciaire préalable pour des raisons d'efficacité, en intervenant en amont du recrutement des candidats pour les empêcher d'accéder aux contenus de propagande et aux sites de recrutement. Il ne fait pas la distinction entre l'efficacité contre le recrutement terroriste et la communication face à la propagande terroriste. Ces deux problématiques appellent pourtant des réponses de nature différente.

D'après les explications obtenues au sujet du projet de loi, le dispositif proposé vise plus particulièrement à donner à l'administration les moyens d'agir dans l'urgence face à la grande viralité des contenus et des sites, alors qu'une décision judiciaire est aujourd'hui nécessaire pour bloquer chaque réplique des contenus.

[1] Voir l'avis n°2013-4 sur la proposition de loi renforçant la lutte contre le système prostitutionnel (http://www.cnnumerique.fr/avis-prostitution/), l'avis n°2013-6 du 17 décembre 2013 sur les contenus et les comportements illicites en ligne (http://www.cnnumerique.fr/contenus-illicites/) et l'avis n°2013-5 du 6 décembre 2013 sur les libertés numériques (http://www.cnnumerique.fr/libertes-numeriques/).

Or, il ressort des autres auditions qu'une distinction doit être opérée entre le recrutement et l'activation, et que les processus d'attraction sont lents et progressifs. Les cibles passent le plus souvent par de nombreuses phases d'endoctrinement et d'intégration avant d'être incitées à passer à l'acte ou à rejoindre un groupe. De l'avis de plusieurs professionnels de la lutte antiterroriste, ces sites de recrutement sont peu nombreux et la décision de les bloquer doit être mise en balance avec l'intérêt de les surveiller.

Enfin, les contenus sont de nature très diverse et complexe. Ils nécessitent une expertise et un contrôle attentifs afin de déterminer ce qui relève de la provocation au terrorisme et ce qui relève de l'opinion. Ils sont surtout diffusés pendant les phases de sensibilisation qui précèdent le recrutement. Ils sont échangés loin du cœur des communautés activistes, non pas sur des sites au sens propre, mais sur des plateformes ou dans des forums dans lesquels se côtoient contenus licites et illicites. Pour être efficace, un dispositif de blocage devrait être capable d'analyser finement le contenu même de ces échanges personnels. Ces techniques d'inspection profonde relèveraient non seulement de la censure, mais aussi de l'atteinte à la vie privée et à la liberté de conscience, et seraient inadmissibles en tant que telles.

Le Conseil est d'avis que

1. Le dispositif de blocage proposé est techniquement inefficace

- Les dispositifs de blocage auprès des FAI sont facilement contournables par les recruteurs comme par les internautes puisqu'ils ne permettent pas de supprimer le contenu à la source[2].

- Le dispositif proposé présente le risque de pousser les réseaux terroristes à complexifier leurs techniques de clandestinité, en multipliant les couches de cryptage et en s'orientant vers des espaces moins visibles du réseau, renforçant la difficulté du travail des enquêteurs. Certaines de ces techniques sont très faciles à utiliser et sont déjà maîtrisées par les tranches d'âge cibles des recruteurs, qui sont familiers de l'usage des Réseaux Privés Virtuels (VPN), du Peer-to-Peer (P2P) ou de TOR.

- Le dispositif proposé risque d'être contreproductif en termes d'image et de pédagogie. Etant facilement contournable, il pourrait laisser penser que les autorités sont « *en retard* » dans la guerre technologique, aboutissant ainsi à créer un sentiment de fierté et d'impunité.

- Comme le montre le rapport des députées Corinne Erhel et Laure de la Raudière, en l'état des techniques actuelles, les dispositifs de blocage par l'accès présentent des risques de sur-blocage et de sous-blocage. Les expériences infructueuses de pays comme le Royaume-Uni[3], les Etats-Unis[4] ou l'Australie confirment ce risque. Un même serveur pouvant héberger plusieurs sites ou contenus parfaitement légaux, leur blocage collatéral constitue une atteinte directe à la liberté d'expression et de communication. La seule solution serait d'inspecter directement et massivement le contenu des communications des internautes[5], faisant ainsi peser des risques graves en matière de respect de la vie privée et de la liberté de conscience.

---

[2] De nombreuses techniques permettent d'échapper au filtrage d'internet: serveurs mandataires (proxy), tunnels, changement d'hébergement ou rotation des URL, Botnets, changement de DNS...

[3] En Grande-Bretagne où les FAI appliquent désormais un filtrage par défaut à la demande du gouvernement, près de 20% des sites les plus populaires sont bloqués par au moins un opérateur télécom, dont seulement 4% de sites pornographiques.

[4] Aux Etats-Unis, le blocage de 10 sites pédopornographiques par les autorités américaines avait causé le blocage de 84 000 sites légaux partageant le même fournisseur DNS.

[5] Les opérateurs n'opèrent le blocage qu'au niveau du nom de domaine (DNS), éventuellement au niveau du sous nom de domaine. Tout blocage plus fin (notamment par URL) exigerait des développements techniques plus

2. Le dispositif proposé est inadapté aux enjeux de la lutte contre le recrutement terroriste

- ***Le principe du recours à une autorité judiciaire préalable reste indispensable :***

    - Les consultations conduites par le Conseil ont mis en évidence que le nombre de sites de recrutement se limite à une fourchette comprise entre une dizaine et une centaine, selon les experts. Au regard de ces chiffres, le risque de surcharge des tribunaux parfois évoqué n'est pas caractérisé et il n'apparait pas raisonnable de créer un dispositif spécifique contournant l'autorité judiciaire au profit de l'autorité administrative.

    - Le dispositif proposé comporte un risque important de télescopage entre l'activité des autorités administratives et celle des services judiciaires. Par exemple, la fermeture intempestive d'un site ou d'un contenu par l'administration pourrait alerter les terroristes de la surveillance judiciaire dont ils font l'objet.

    - Le dispositif proposé ne tient pas compte des retours négatifs et des risques soulevés par les expériences similaires à l'étranger, notamment en ce qui concerne la lutte contre le terrorisme aux Etats-Unis, les révélations d'Edward Snowden à ce sujet et le risque de perte de confiance des consommateurs dans l'écosystème numérique.

- ***Les dispositifs de blocage ne sont pas une réponse à la compétition pour l'attention et l'influence, sur les populations visées par les filières terroristes, en particulier les jeunes :***

    - Il apparaît illusoire d'adresser les dynamiques de propagation d'images et de contenus propres au Web et aux réseaux sociaux par des mesures techniquement contournables. A cet égard, la seule hypothèse où le dispositif serait efficace relève d'une exploitation massive et automatisée, en désaccord flagrant avec les principes d'un Etat de droit.

    - Dans un contexte de lutte contre les stratégies de diffusion d'idéologies radicales, le recours au blocage peut avoir un effet contreproductif en attisant l'envie de consulter les contenus bloqués.

Recommandation - Les acteurs consultés soulèvent la nécessité de développer la recherche pour mieux comprendre la dimension sociale de la radicalisation et déterminer précisément le rôle d'Internet dans ce processus. De nombreux facteurs peuvent concourir au basculement d'individus dans la violence tout en étant étrangers à la provocation directe aux actes terroristes ou à leur apologie. Le contact avec des idéologies extrémistes peut se produire sur Internet comme en dehors des sphères numériques. La recherche sur ces sujets mérite d'être renforcée afin de pouvoir servir de fondement à toute future décision.

Recommandation - Dans une optique de prévention, les mêmes experts pointent l'importance particulière de l'éducation et du développement de capacités d'interprétation critique des divers messages véhiculés - dans l'environnement numérique comme en dehors.

---

importants et nécessiterait d'avoir recours aux techniques de *deep packet inspection* (DPI), particulièrement attentatoire au secret des correspondances.

3. Le dispositif proposé n'offre pas de garanties suffisantes en matière de libertés

- Afin de maintenir l'autorité judiciaire dans le processus, le dispositif proposé prévoit la désignation, par le Garde des sceaux, d'un magistrat de l'ordre judiciaire, dont le contrôle portera sur la régularité des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste des adresses électroniques des services de communication au public en ligne.

- Ces mesures ne sont pas suffisantes pour une double raison :

    - ce magistrat n'est pas en charge du contrôle de l'opportunité du blocage lui-même ;
    - nommé par le gouvernement, il ne dispose pas des garanties d'indépendance offertes par le processus judiciaire.

- Le Conseil constitutionnel a rappelé que le blocage d'un site Internet constitue une atteinte grave à la liberté d'expression et de communication[6]. Toute atteinte aux libertés, fût-elle justifiée par des considérations de sécurité nationale, doit être proportionnée et nécessaire vis-à-vis de l'objectif recherché. Or, le dispositif proposé met en place une procédure exceptionnelle de blocage administratif sans que celle-ci soit justifiée par des conditions comme l'urgence imminente ou l'absence de toute autre solution disponible.

- Contrairement aux dispositions relatives à la pédopornographie, il ressort des consultations effectuées par le Conseil que la qualification des notions de commission d'actes terroristes ou de leur apologie prête à des interprétations subjectives et emporte un risque réel de dérive vers le simple délit d'opinion.

Recommandation **-** La multiplication du recours à des régimes d'exception propres à isoler le numérique participe à appauvrir la cohérence des lois. Le Conseil recommande en ce sens d'instaurer un **moratoire** sur l'ensemble des projets de dispositions instituant des mesures de blocage ou de filtrage sur Internet. L'arbitrage entre les impératifs de sécurité et de liberté devrait être effectué avec prudence, dans un cadre préservé des pressions de l'actualité.

La multiplication de ces dispositifs depuis 2004 nécessite de **dresser un bilan et d'analyser leur efficacité**. Sur ce sujet, encore plus que sur les autres sujets numériques, le Conseil encourage à effectuer des études de besoin et d'impact chiffrées, en volume, délais, coûts, risques, conséquences pour les professionnels du secteur, etc. voire même des simulations.

Recommandation **-** De façon générale, un tel dispositif devrait proposer des outils permettant de mesurer son efficacité, comme des indicateurs ou des dates butoir permettant de réexaminer les mesures mises en œuvre.

[6] Décision n° 2011-625 du 10 mars 2011.

4. Il est possible d'utiliser des alternatives plus efficaces et plus protectrices que le blocage administratif auprès des FAI

- D'autres secteurs offrent des exemples de mécanismes hybrides qui articulent efficacement les autorités administrative et judiciaire tout en apportant tous les garde-fous nécessaires. Le système de signalement de l'ARJEL[7] permet par exemple à son Président de soumettre des séries de sites à bloquer au Président du Tribunal de grande instance qui les examine à intervalles réguliers. Cela permet de préserver le rôle d'un juge spécialisé dans la prise de décision. L'action des deux autorités est coordonnée et la régularité des audiences permet des délais suffisamment rapides.

Recommandation **-** Un dispositif similaire pourrait être étudié entre l'autorité l'administrative et les autorités judiciaires antiterroristes. Il pourrait par exemple permettre aux autorités administratives de présenter à dates régulières des séries de sites et de contenus à l'autorité judiciaire pour demander leur blocage, tout en utilisant une procédure spécifique de référé ou des mesures conservatoires dans les situations d'extrême urgence.

- Il existe également d'autres solutions pour pallier les lourdeurs inhérentes à la nécessité d'obtenir une décision judiciaire à chaque nouvelle apparition d'un site « *miroir* ». Le rapport interministériel sur la lutte contre la cybercriminalité[8] recommande par exemple de maintenir le rôle de l'autorité judiciaire, mais d'accompagner la décision du juge d'une obligation de surveillance spécifique mise à la charge de l'opérateur et limitée dans le temps, destinée à prévenir, dans la mesure du possible, les procédés de contournement et la duplication de sites ou contenus illicites.

Recommandation **-** Dans un registre plus respectueux de l'esprit de l'économie numérique, il serait également possible de mettre en place une procédure judiciaire accélérée en ce qui concerne les simples réplications de contenus déjà condamnés.

- Par ailleurs, le dispositif proposé crée un régime d'exception pouvant ralentir le développement d'une coopération internationale sur ces sujets. Ce dispositif ne fait que déplacer le problème à l'étranger, entrainant une balkanisation de l'Internet qui pourrait permettre aux recruteurs de jouer entre les différents pays pour se protéger des blocages techniques mis en œuvre localement.

Recommandation **-** Pour être efficace, toute action numérique doit être coordonnée au niveau international, en intégrant le meilleur niveau de garanties possible et en développant des outils concrets comme par exemple un équivalent international de PHAROS - un outil de centralisation du signalement volontaire, une cellule *ad hoc* au niveau européen et/ou de l'OCDE, et des groupes de travail techniques au niveau des organismes de standardisation pour éviter toute balkanisation de l'Internet.

[7] En particulier la possibilité pour l'Autorité de régulation des jeux en ligne (ARJEL) de saisir directement le Président du Tribunal de grande instance (TGI), afin d'ordonner aux hébergeurs et à défaut, aux fournisseurs d'accès Internet, le blocage des sites, et l'instauration d'une systématisation dans l'instruction et l'audiencement des dossiers.
[8] http://www.economie.gouv.fr/remise-du-rapport-sur-la-cybercriminalite

5. En ce qui concerne l'extension du champ des outils de notification, d'autres solutions peuvent être envisagées

Le Conseil appelle à ne pas se reposer sur les seules hypothèses dérogatoires de signalement afin d'éviter la multiplication des régimes d'exception qui limitent le champ d'application du droit commun. Il ne doit jamais être dérogé au principe du recours à une autorité judiciaire préalable avant l'instauration d'un dispositif de surveillance, de suppression ou de blocage de contenus sur Internet.

Recommandation **- Favoriser l'innovation dans l'encadrement des comportements et des contenus illicites au lieu de se reposer sur leur signalement et leur suppression a priori :**

- Standardiser les dispositifs et les procédures d'information et de réaction : améliorer leurs délais de traitement et leur efficacité, faciliter leur repérage pour les internautes, développer un pictogramme unique identique d'une plateforme à l'autre ;

- Améliorer les conditions générales d'utilisation pour vérifier leur lisibilité et la connaissance réelle des droits et des devoirs de leurs utilisateurs, en instaurant un meilleur respect des normes culturelles, linguistiques et sociales ;

- Améliorer les médiations avec les usagers : favoriser la mise en relation des personnes avec des associations mandatées et agréées pour les accompagner, en généralisant la présence de liens de contact visibles ;

- Encourager les bonnes pratiques et faciliter le dialogue entre l'ensemble des acteurs du numérique, les associations de lutte contre les discriminations, ainsi que les utilisateurs d'Internet afin de déterminer ce qui relève des bonnes pratiques, de la législation, de la régulation voire d'une forme de labellisation.

Recommandation **- Généraliser les actions et les outils d'accompagnement, d'éducation, de civisme et de littératie : la responsabilisation des internautes par l'information et l'éducation doit être le préalable à tout autre dispositif d'encadrement :**

- Les outils offerts par Internet peuvent être des supports de sensibilisation et de communication pour tous les publics, par exemple en demandant aux moteurs de recherche ou aux réseaux sociaux de mettre en avant des contenus émanant d'associations de victimes ou en leur offrant des moyens de communication.

- De même, la plateforme PHAROS qui permet de signaler des contenus illicites est par exemple trop méconnue des usagers et pourrait faire l'objet d'une meilleure communication[9].

Recommandation - **Utiliser les outils déjà existants sur les moteurs de recherche, les réseaux sociaux ou les sites de vidéos**. Ils offrent des possibilités bien plus souples et bien plus adaptées que le blocage. Il serait par exemple possible que l'administration procède à de simples demandes de déréférencement de contenus illicites, ou réclame aux plateformes qui ne le font pas encore d'informer PHAROS des contenus qui leur sont signalés.

[9] A l'image des dispositifs mis en place sur les moteurs de recherche pour améliorer la visibilité des services du planning familial.

Recommandation - **Inciter les plateformes à adopter dans leurs propres conditions générales d'utilisation des dispositifs plus équilibrés** comme l'avertissement, la suspension provisoire, ou la mise en place de procédures d'arbitrage interne, en s'inspirant de dispositifs déjà mis en œuvre par les communautés collaboratives en ligne. En ce qui concerne les plateformes qui exercent simultanément en France et à l'étranger, l'administration doit développer des liens réguliers avec elles et le régime qui leur est applicable doit être clarifié.

Annexes

Personnalités auditionnées

ARTIGUELONG Maryse, Membre du comité central de la Ligue des droits de l'Homme, représentante de l'Observatoire des libertés numériques

BAUER Alain, Professeur de criminologie, consultant en sécurité

BOCCIARELLI Eric, Secrétaire général du Syndicat de la Magistrature, représentant de l'Observatoire des libertés numériques

CHARMET-ALIX Adrienne, Coordinatrice générale de la Quadrature du Net, représentante de l'Observatoire des libertés numériques

DELETANG Agnès, Magistrat conseillère auprès du Conseil national du renseignement

FERAL-SCHUHL Christiane, ancien bâtonnier du Barreau de Paris, co-présidente de la Commission Droits et libertés à l'âge du numérique de l'Assemblée nationale

GEORGES Marie, représentante de l'Observatoire des libertés numériques

GHIBELLINI Julie, Administratrice à l'Assemblée nationale

GUERCHOUN Frédéric, Directeur juridique de l'Autorité de régulation des jeux en ligne (ARJEL)

LACOMBE Stéphane, Chef de projet et consultant pour l'Association française des victimes du terrorisme

MANACH Jean-Marc, Journaliste d'investigation

MOURTON Mathieu, Administrateur à l'Assemblée nationale

QUÉMÉNER Myriam, Avocat général près la Cour d'appel de Versailles

RABENOU Jérôme, Adjoint au directeur général délégué aux contrôles et aux systèmes d'information de l'Autorité de régulation des jeux en ligne (ARJEL)

TRÉVIDIC Marc, Juge d'instruction au Tribunal de grande instance de Paris au pôle antiterrorisme

WARUSFEL Bertrand, Avocat spécialisé sur les questions de sécurité, professeur à l'université Lille 2

WIEVORKA Michel, Sociologue spécialisé dans le terrorisme

ZABULON Alain, Coordinateur national du renseignement

Ressources documentaires

Quiliam, *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it,* Ghaffar Hussain and Dr. Erin Marie Saltman, May 2014
Disponible ici : http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/jihad-trending-quilliam-report.pdf
Résumé : http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/djihad-trending-sur-internet.pdf

Rapport d'information n°3336 du 13 avril 2011 de MM. Corine Erhel et Laure de la Raudière sur la neutralité de l'Internet et des réseaux
Disponible ici : http://www.assemblee-nationale.fr/13/rap-info/i3336.asp

Rapport n°2000 du 4 juin 2014 sur la proposition de loi n°1907 de MM. Guillaume Larrivé, Eric Ciotti, Philippe Goujon et Olivier Marleix renforçant la lutte contre l'apologie du terrorisme sur Internet
Disponible ici : http://www.assemblee-nationale.fr/14/rapports/r2000.asp

Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a changing world,* 12 December 2013 :
Disponible ici : http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Aconite Internet Solutions, *Internet blocking: balancing cybercrime responses in democratic societies,* Cormac Callanan (Ireland), Marco Gercke (Germany), Estelle De Marco (France), Hein Dries-Ziekenheiner (Netherlands), October 2009
Disponible ici : http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf
Synthèse en français :
http://www.laquadrature.net/files/Filtrage_d_Internet_et_d%C3%A9mocratie%20-%20R%C3%A9sum%C3%A9%20Principal_1.pdf