Entre sécurité et liberté, quel équilibre pour la défense et la sécurité de l'espace numérique ?

par Marc WATIN-AUGOUARD

Général d'armée (2S), Directeur du centre de recherches de l'Ecole des Officiers de la Gendarmerie nationale (EOGN)

Fondateur du Forum International de la Cybersécurité (FIC)

La symbiose entre la sécurité et la liberté est au cœur de la construction de l'État de droit. L'une ne va pas sans l'autre ; loin de s'opposer elles se composent. La jurisprudence du Conseil constitutionnel, celle du Conseil d'Etat, de la Cour EDH ou de la CJUE témoignent d'une recherche d'équilibre entre les exigences de sécurité et celles de liberté.

Si les grands principes semblent stabilisés s'agissant du « monde réel », l'émergence des nouvelles technologies qui accompagnent le développement de l'espace numérique pose les problèmes en de nouveaux termes. Il est intéressant de noter que le cyberespace est d'abord né des exigences de sécurité et de défense avec le programme lancé à la fin des années cinquante par Paul Baran. Abandonné, il a cédé la place à des équipes universitaires n'ayant qu'une seule idée en tête, celle de liberté. On peut même parler de courant libertaire soutenu par le « néocommunalisme » américain et les 750 000 hippies, vivant pour la plupart dans la *Silicon Valley*, mais, pour nombre d'entre eux, doctorants dans les grandes universités américaines …

Avec quelques dizaines ou centaines de machines connectées, « l'indépendance du cyberespace » aurait pu demeurer une sympathique utopie. Mais avec plus de dix milliards de machines en 2017 et peut-être mille milliards en 2030, l'espace numérique cesse d'être « ailleurs ». A terme, il formera sans doute le seul espace qui se déclinera selon le milieu terrestre, maritime ou aérien.

Dès le début de la démocratisation du cyberespace, arrive le prédateur et, avec lui, commencent à s'élaborer des stratégies de sécurité et de défense, d'abord avec la lutte contre la cybercriminalité puis, plus récemment, avec la cyberdéfense. L'espace numérique apparaît de plus en plus comme un espace propice au profit, à la compétition, à la propagande, à l'influence, voire à la

conflictualité. Cet espace est souvent représenté par ses trois « couches » : la couche « matérielle », la couche « logicielle ou logique » et la couche « sémantique ou cognitive ».

La première constitue l'ancrage du cyberespace dans le monde réel. C'est par elle que l'on entre, que l'on sort ou que l'on transite dans l'espace numérique. Elle est constituée des infrastructures, routeurs, câbles sous-marins, data centers, etc. qui peuvent être l'objet de malveillances. Leur sécurité est une condition de leur fonctionnement et donc du libre accès au réseau. Cette couche ne présente pas de spécificité par rapport aux mesures de sécurité et aux éventuelles restrictions de liberté qui s'appliquent aux infrastructures du monde réel.

La liberté de la couche logique appelle des mesures de sécurité pour le moment assez peu intrusives dans la vie privée. On notera cependant que sa protection passe de plus en plus par des analyses de flux, par des profilages de requêtes. La cybersécurité ne doit pas avoir d'autre objectif que celui de garantir un espace numérique sécurisé.

Si la couche « logique » de l'espace numérique demeure un objectif privilégié des cyberattaquants, la couche « sémantique » ou « cognitive », celle du sens, offre aux prédateurs un champ d'action de plus en plus vaste, ne serait-ce qu'en raison de la croissance démographique d'internet : 3 ,7 milliards d'internautes en 2017, 5 milliards prévus en 2025. Les données sont désormais la cible principale des prédateurs en tout genre, en raison de leur valeur intrinsèque, des multiples possibilités qu'elles offrent, dès lors qu'elles sont « *volées, dénaturées, prises en otage, manipulées, etc.* ». Elles sont aussi pour les enquêteurs et pour les agents des services de renseignement un objet de recherches souvent très intrusives dans la vie privée par le biais des techniques spéciales d'enquête ou des techniques de renseignement[1].

Au sein de cette couche, la sécurité et la liberté entrent parfois en opposition, comme en témoignent notamment les débats qui ont accompagné et suivi l'élaboration de la loi du 24 juillet 2015, relative au renseignement, et des lois de sécurité qui comportent toutes désormais des dispositions concernant le cyberespace[2]. Les contenus sont généralement conformes à la loi. Les deux milliards de comptes *Facebook* et les plus de quatre milliards de comptes de messagerie sont heureusement pour la plupart dans les mains d'internautes respectueux des règles imposées. Mais les contenus sont aussi parfois illicites : trafic de produits réglementés, offres de contrefaçons, propos ou images contraires aux dispositions de la loi du 27 juillet 1881 (diffamation, injures, provocation publique à la haine, la violence ou la discrimination raciale, diffusion de fausses nouvelles troublant la paix publique, etc.),

1. Voir Marc Watin-Augouard, « Les investigations judiciaires dans le cyberespace », *in ADSD*, 2016.
2. Par exemple, les lois successives sur l'état d'urgence ou la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

atteintes à la vie privée, diffusions de fausses nouvelles ou de rumeurs[3]. Le législateur a donc complété le corpus pénal en portant tout particulièrement son attention sur les contenus à caractère pédophile et, plus récemment, sur les contenus à caractère terroriste. Seuls ces derniers sont ici examinés[4], car ils sont la parfaite illustration de « l'opposition de phase » entre la sécurité et la liberté[5]. L'accroissement de leur répression, depuis 2014 et singulièrement depuis les attentats de 2015, témoigne d'une volonté de combattre un terrorisme qui manie les réseaux sociaux avec un très grand professionnalisme (**I**). La tentation de répondre au terrorisme par voie législative a néanmoins été tempérée par le juge constitutionnel qui s'est montré particulièrement soucieux de protéger la liberté de communication et d'expression (**II**). L'équilibre entre la sécurité et la liberté ne peut être que le résultat d'une gouvernance des contenus qui, sans nier l'importance de l'État, repose sur un dialogue constructif entre la puissance publique et les médias sociaux (**III**).

I. Une accentuation de la répression des contenus à caractère terroriste

Internet est devenu le principal vecteur de propagation des appels à la commission d'actes de terrorisme. « *Les groupes terroristes maîtrisent parfaitement toutes les potentialités de l'espace numérique, diffusant des messages de propagande généralement bien conçus et incisifs, traduits dans toutes les langues, et s'appuyant sur l'ensemble des volontaires ralliés à travers leurs propres pages ou comptes (Facebook, Twitter) qui démultiplient de manière exponentielle l'appel au ralliement* »[6].

En 2013, 122 sites ont fait l'objet d'un signalement pour apologie du terrorisme. La diffusion sur internet, depuis août 2014, de la décapitation de

3. L'article L. 465-2 alinéa 2 du code monétaire et financier institue un délit qui consiste à répandre dans le public par des voies et moyens quelconque, communiqué de presse, conférence, des informations fausses ou trompeuses sur les perspectives ou la situation d'un émetteur dont les titres sont négociés sur un marché réglementé ou sur les perspectives d'évolution d'un instrument financier admis sur un marché réglementé, ces informations doivent être de nature à agir sur les cours. L'article L. 97 du code électoral permet de condamner ceux qui, à l'aide de fausses nouvelles, bruits calomnieux ou autres manœuvres frauduleuses, auront surpris ou détourné des suffrages, déterminé un ou plusieurs électeurs à s'abstenir de voter, seront punis d'un emprisonnement d'un an et d'une amende de 15 000 euros. Il est souvent difficile de prouver que des suffrages ont été détournés à cause de la fausse nouvelle. Pour le Conseil d'État, une fausse nouvelle, de nature à créer une confusion dans l'esprit des électeurs et à porter atteinte à la sincérité du scrutin, emporte annulation de l'élection.

4. L'intervention orale lors du colloque de Lille couvrait un champ plus large, mais l'actualité juridique du dernier trimestre 2017 justifie un recentrage sur le terrorisme et l'incorporation de faits et textes qui lui sont postérieurs.

5. Nous employons cette image par référence à la pile : sécurité et liberté sont comme les pôles d'une pile électrique ; tout semble les opposer alors qu'il n'y a pas de lumière sans l'un et l'autre.

6. Assemblée Nationale, rapport de Sébastien Pietrasanta, fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République. Travaux parlementaires relatifs à loi du 13 novembre 2014.

plusieurs otages[7], dont celle, en Algérie, du français Hervé Gourdel ont particulièrement sensibilisé l'opinion publique et le législateur. Les attentats de 2015 vont prouver qu'il ne s'agit alors que des prémices, puisque, dans les heures qui suivent l'attentat contre Charlie Hebdo, ce sont près de 20.000 sites qui sont défacés en France pour servir de propagande à Daesh.

C'est pourquoi le gouvernement va durcir la législation relative aux contenus terroristes. Le transfert de la provocation au terrorisme et de son apologie vers le code pénal va renforcer la répression de cette infraction à laquelle s'ajoute l'interdiction de la fabrication, du transport et de la diffusion de messages à caractère terroriste (**A**). Mais la création d'une infraction de consultation habituelle de sites à caractère terroriste va faire l'objet d'une double censure du Conseil constitutionnel (**B**).

A. Le transfert vers le code pénal de la provocation au terrorisme et de son apologie

Robert Badinter, que l'on ne peut qualifier de « liberticide », soulignait déjà lors des débats au Sénat en 2004 que *« la technique a fondamentalement modifié les données du problème. [...] Nous ne sommes plus au temps de la presse imprimée ! Nous sommes tous ici des défenseurs de la liberté de la presse et j'ai, pour ma part, beaucoup plaidé pour elle au cours de ma vie. Mais nous sommes là devant un outil qui est sans commune mesure avec la presse écrite que nous avons connue, et qui était en fait celle de 1881. L'internet pose des problèmes considérables et il faut prendre des dispositions adaptées* » [8].

Avec la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, la provocation aux actes de terrorisme ou leur apologie ne relèvent plus de la loi du 29 juillet 1881 sur la liberté de la presse (article 24) mais deviennent des infractions terroristes. Ces infractions sont aggravées lorsqu'elles sont commises à l'aide d'un moyen de communication électronique en ligne[9], ce qui souligne la plus grande nocivité du message transmis par cette voie. Un site internet n'a, dans les faits, qu'un lointain rapport avec celui d'un organe de presse, ce qui montre bien l'inadaptation de la loi de 1881 aux contenus véhiculés par internet. L'article 421-2-5 du code pénal réprime désormais le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes. La peine, initialement fixée par l'article 24 de la loi du 29 juillet 1881, à 5 ans d'emprisonnement, est maintenue mais est portée à 7 ans d'emprisonnement lorsque les faits sont commis sur internet.

---

7. Le journaliste américain James Foley et le britannique Alan Henning ont été les premières victimes de Daech en Syrie.
8. Sénat, 20 janvier 2004, débat sur le projet de loi portant adaptation de la justice aux évolutions de la criminalité.
9. Le Sénat ne voulait opérer ce transfert que dans le seul cas d'un recours à un moyen de communication électronique en ligne, mais il n'a pas été suivi par la commission paritaire.

Pour Manuel Valls, alors ministre de l'intérieur, ces infractions « *ne constituent plus seulement un usage abusif de la liberté d'expression mais un acte grave inscrit dans une stratégie de combat participant d'une activité terroriste à part entière*[10] ».

La provocation doit être une incitation directe, par son esprit comme par sa lettre, à commettre des actes de terrorisme matériellement déterminés. Le critère de la publicité n'est pas exigé par la loi, car la provocation non publique est réprimée : sont donc aussi concernés les prêches dans les lieux non ouverts au public, les réunions privées, les réseaux sociaux accessibles à un nombre restreint de personnes agréées. En revanche, l'apologie « privée » n'est pas réprimée. Celle-ci consiste à présenter ou commenter des actes de terrorisme en portant sur eux un jugement moral favorable. La condition de publicité, prévue par l'article 23 de la loi sur la liberté de la presse est exigée pour caractériser l'infraction.

Le transfert vers le code pénal a une valeur qui dépasse le symbole, puisqu'il a des incidences sur des règles de procédure exclues en matière de presse: possibilité de convocation par procès-verbal ou de comparution immédiate, application du régime procédural dérogatoire prévu par le code de procédure pénale en matière de terrorisme, sauf en ce qui concerne le délai de prescription (prescription[11] de trois ans et non plus d'un an pour les mêmes infractions lorsqu'elles étaient sous le régime de la loi sur la liberté de la presse), les perquisitions de nuit et les règles particulières de garde à vue[12]. En novembre 2014, le législateur ignorait que ce nouvel article aurait une application aussi rapide et aussi démultipliée, redonnant à la plupart des tribunaux correctionnels une compétence pour des affaires de terrorisme, jusqu'alors presque toutes attraites par le parquet de Paris.

Enfin, complément naturel de l'article précité, l'article 227-24 du code pénal (modifié par l'article 7 de la loi du 13 novembre 2014), s'alignant sur le régime des contenus à caractère pornographique, réprime le fait « *soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent, incitant au terrorisme* ».

---

10. Assemblée nationale, 27 novembre 2012, débats sur loi n°2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme.

11. Le point de départ du délai de prescription est la publication ou la diffusion du document en cause ou sa mise en ligne.

12. L'article 706-24-1 du code de procédure pénale (créé par l'article 8 de la loi renforçant les dispositions relatives à la lutte contre le terrorisme) dispose que les articles 706-88 à 706-94 du code de procédure pénale ne sont pas applicables aux délits prévus à l'article 421-2-5 du code pénal. Selon le même article, l'article 706-25-1 n'est pas non plus applicable. Le Conseil constitutionnel considère que les techniques spéciales d'enquête ne doivent être mises en œuvre que pour les infractions les plus graves. Cons. const., déc. n° 2004-492 DC du 2 mars 2004 : « Si le législateur peut prévoir des mesures d'investigation spéciales en vue de constater des crimes et délits d'une gravité et d'une complexité particulières, d'en rassembler les preuves et d'en rechercher les auteurs, c'est sous réserve que les restrictions qu'elles apportent aux droits constitutionnellement garantis soient nécessaires à la manifestation de la vérité, proportionnée à la gravité et à la complexité des infractions commises et n'introduisent pas de discrimination injustifiée ». Voir également Cons. const., déc. n° 2013-679 DC du 4 décembre 2013 et déc. n°2014-420/421 QPC du 9 octobre 2014.

La peine prévue est de trois ans d'emprisonnement et 75 000 euros d'amende.

B. La consultation habituelle de sites à caractère terroriste, infraction autonome

La consultation habituelle de sites à caractère terroriste est d'abord retenue dans la législation comme élément constitutif de l'infraction d'entreprise terroriste individuelle (**1**) Puis, malgré l'opposition du gouvernement, elle est érigée en infraction autonome par la loi du 6 juin 2016 (**2**).

1. Un élément constitutif de l'infraction d'entreprise individuelle

S'agissant des contenus à caractère terroriste, la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme ne crée pas une incrimination semblable à celle qui est en vigueur pour les sites pédopornographiques (qui pénalise directement la consultation habituelle de sites). Mais celle-ci fait partie de la liste des faits matériels qui, avec d'autres, sont les indices constitutifs de l'infraction d'entreprise individuelle définie par le nouvel article 421-2-6 du code pénal.

Le texte voté par l'Assemblée nationale excluait la responsabilité pénale lorsque la consultation ou la détention résulte de l'exercice normal d'une profession ayant pour objet d'informer le public, intervient dans le cadre de recherches scientifiques ou a pour objet de servir de preuve en justice. Ces exclusions ne sont plus mentionnées dans la loi promulguée, laissant au juge le soin d'apprécier le contexte d'une telle consultation et en premier lieu l'intention terroriste de leur auteur.

2. La création d'une infraction autonome fragile dès sa conception

La consultation habituelle d'un service de communication au public en ligne mettant à disposition des messages, images ou représentations, soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes est finalement incriminée par la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale. Jean-Jacques Urvoas, garde des sceaux, s'y était opposé à l'occasion des débats, arguant que la consultation de sites djihadistes est déjà l'un des critères constitutifs d'une entreprise individuelle terroriste. Le droit en vigueur suffisait donc, selon lui, pour atteindre les objectifs visés par les auteurs de l'amendement. Lors des débats, le rapporteur du texte à l'Assemblée nationale, Pascal Popelin, avait lui-même émis des doutes sur sa constitutionnalité. Malgré ces fortes réserves, le texte est voté. Il n'est pas soumis aux Sages par voie d'action. Il le sera par voie d'exception sur renvoi d'une question prioritaire de constitutionnalité (QPC) transmise par la Cour de cassation.

II. La sanction constitutionnelle d'un déséquilibre entre la sécurité et la liberté

Le texte issu de la loi du 3 juin 2016 est déclaré contraire à la constitution par décision QPC du 10 février 2017 (**A**). Quelques jours plus tard, dans le cadre de l'examen de la loi pour la sécurité publique, la commission mixte paritaire rétablit un article prenant en compte, selon ses auteurs, les considérants du Conseil constitutionnel (**B**). Finalement, saisi par une QPC, le Conseil constitutionnel déclare à nouveau le délit de consultation habituelle contraire à la Constitution[13](**C**).

A. La première censure par le Conseil constitutionnel

L'article 421-2-5-2 C. pén. est censuré par la Conseil constitutionnel, après saisine par QPC transmise par la Cour de cassation.

La Cour considère, en effet, que cet article pose question :

- En ce qu'il incrimine et punit la consultation habituelle sans définir les critères permettant de qualifier une consultation d'habituelle, prévoit une exception de bonne foi sans en définir les contours et n'apporte aucune définition de la notion de terrorisme,

- En ce qu'il atteint à la liberté de communication et d'opinion de tout citoyen en punissant d'une peine privative de liberté la seule consultation de messages incitant au terrorisme, alors même que la personne concernée n'aurait commis ou tenté de commettre aucun acte pouvant laisser présumer qu'elle aurait cédé à cette incitation ou serait susceptible d'y céder,

- En ce qu'il crée une rupture d'égalité entre les personnes ayant accès à de tels messages, images ou représentations par un service de communication en ligne et celles y ayant accès par d'autres moyens et supports qu'un service de communication en ligne,

- En ce qu'il crée une rupture d'égalité entre les citoyens souhaitant bénéficier d'un accès à de tels services et ceux dits "de bonne foi" ou autorisés expressément par la loi,

- En ce qu'il punit de deux années d'emprisonnement et de 30 000 euros d'amende la seule consultation, même habituelle, d'un service de communication en ligne,

- En ce qu'il institue une présomption de mauvaise foi déduite de la seule consultation de ces services de communication en ligne ».

Le Conseil constitutionnel, s'appuyant sur l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 considère « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise*

13. Cons. const., déc. n° 2017-682 QPC du 15 décembre 2017.

par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions » la libre communication des pensées et des opinions est un droit qui implique l'accès à ces services. Cette liberté de communication implique la liberté de diffuser et la liberté de recevoir des idées.

Les atteintes à l'exercice de cette liberté doivent donc être nécessaires, adaptées et proportionnées à l'objectif poursuivi. C'est sur cette trilogie que le Conseil se fonde pour censurer le texte.

Tout d'abord, la nécessité de l'article contesté n'est pas fondée. Selon les Sages, la législation comprend un ensemble d'infractions pénales autres que celle prévue à l'article 421-2-5-2 qui permettent d'agir (association de malfaiteurs, provocation à la commission d'actes de terrorisme ou leur apologie, entreprise individuelle de terrorisme, etc.). Elle confère également de nombreux pouvoirs et capacités d'action à l'autorité administrative dans le cadre de la loi sur le renseignement (techniques spéciales de renseignement – Livre VIII titre V du CSI). En matière de retrait, de blocage ou de déréférencement des sites à caractère terroriste, l'autorité judiciaire (art. 706-23 du CPP) et l'autorité administrative (art. 6-1 de la loi pour la confiance dans l'économie numérique) ne sont pas dépourvues de moyens d'action. Le Conseil constitutionnel considère donc que la justice et les services de police et de gendarmerie disposent de suffisamment de moyens juridiques pour lutter contre des consultations de sites à caractère terroriste.

L'adaptation et la proportionnalité sont contestées par la Conseil au motif que l'infraction punie d'une peine de deux ans d'emprisonnement est indépendante de toute volonté de commettre un acte terroriste ou de toute adhésion à l'idéologie portée par les sites visés. Elle fait peser une incertitude sur la licéité de leur consultation. En effet, la « bonne foi » censée exclure la pénalisation n'est guère explicitée par le texte ou par les travaux parlementaires. Ses contours sont trop flous.

Avant d'être reprise par la loi du 3 juin 2016, l'incrimination avait été adoptée en première lecture par le Sénat statuant le 2 février 2016 sur une proposition de loi. Ceci explique son introduction en première lecture au Sénat. Son maintien après la commission mixte paritaire est sans aucun doute l'illustration d'une recherche de consensus sur le texte entre les deux assemblées.

Chronique d'une inconstitutionnalité annoncée ! Lors de l'examen d'un projet de loi renforçant la prévention et la répression du terrorisme (projet déposé le 11 avril 2012 et caduc après les élections), la Conseil d'État, saisi pour avis, avait considéré que « *de telles dispositions, sans véritable précédent dans notre législation ni équivalent dans celles des autres États membres de l'Union européenne, permettaient d'appliquer des sanctions pénales, y compris privatives de liberté, à raison de la seule consultation de messages incitant au terrorisme, alors même que la personne concernée n'aurait commis ou tenté de commettre aucun acte pouvant laisser présumer*

qu'elle aurait cédé à cette incitation ou serait susceptible d'y céder ». Le Conseil d'État a considéré que de telles dispositions *« portaient à la liberté de communication, dont une protection particulièrement rigoureuse est assurée tant par le Conseil constitutionnel que par la Cour européenne des droits de l'homme, une atteinte qui ne pouvait être regardée comme nécessaire, proportionnée et adaptée à l'objectif de lutte contre le terrorisme* ».

Cette inconstitutionnalité, notons-le, n'a pas d'impact sur le délit de consultation habituelle de site pédophile, tant cette infraction ne souffre, hélas, d'aucune ambiguïté.

B. La réécriture lors de l'examen de la loi sur la sécurité publique

Malgré les opinions émises par Pascal Popelin, rapporteur de la loi du 3 juin 2016 qui avait alors exprimé publiquement des réserves sur la constitutionnalité de l'article, la commission mixte paritaire, réunie pour finaliser la loi sur la sécurité publique du 28 février 2017, adopte un nouvel article, dont la rédaction selon son auteur, le sénateur Philippe Bas, devait répondre aux conditions posées par le Conseil constitutionnel. La loi corrige un certain nombre d'imperfections ayant motivé la censure du texte précédent. Répond-elle à l'exigence de nécessité ? Pour Philippe Bas, « *c'est précisément lorsque le ministère public et le tribunal correctionnel n'ont pas d'éléments démontrant qu'un individu met en œuvre une entreprise individuelle à des fins terroristes, ou participe à une association de malfaiteurs en vue de commettre un attentat terroriste, que ce délit est utile* ».

Le nouveau texte ne sanctionne plus la simple consultation : il faut qu'elle soit habituelle (inchangé) et s'accompagne en plus « *d'une manifestation de l'adhésion à l'idéologie exprimée sur ce service* ». C'est une reprise mot à mot d'un des considérants de la décision QPC. Par ailleurs, il définit la notion de « motif légitime », lequel est caractérisé « *notamment* » en cas de « *consultation résultant de l'exercice normal d'une profession ayant pour objet d'informer le public, intervenant dans le cadre de recherches scientifiques ou réalisée afin de servir de preuve en justice ou le fait que cette consultation s'accompagne d'un signalement des contenus de ce service aux autorités publiques compétentes* ». Selon les travaux parlementaires, l'individu qui consulte régulièrement de tels sites, mais qui « prend le soin d'en dénoncer l'existence aux officiers de police judiciaire », ne sera pas poursuivi.

La nature de la manifestation de l'adhésion à l'idéologie n'est pas précisée. La difficulté, comme le souligne le député Dominique Raimbourg, c'est de définir ce qu'est la « *manifestation de l'adhésion à l'idéologie exprimée* » sur le service que consulte l'intéressé sur son ordinateur : « *S'il est tout seul devant celui-ci, comment caractériser cette manifestation ? S'il n'est plus*

seul, il relève de l'apologie du terrorisme[14] *».* Le rapport de la commission mixte paritaire évoque, par exemple, « *des correspondances avec des tiers les invitant à consulter ces mêmes sites ou faisant part de l'adhésion à cette idéologie, ou le fait que, pendant une perquisition, on trouve certains objets qui attestent de l'adhésion de l'individu à cette idéologie* ».

N'ayant pas été déférée devant le Conseil constitutionnel par les voies directes, la loi fait l'objet d'une QPC transmise à nouveau par la Cour de cassation, le 4 octobre 2017[15] .

C. La QPC du 4 octobre 2017 ou l'inconstitutionnalité définitive du délit.

La Cour de cassation est saisie de l'examen d'une QPC qui repose sur plusieurs arguments : L'article 421-2-5-2 est-il conforme à la Constitution ? :

- En ce qu'il a été réintroduit par le législateur malgré une décision rendue par le Conseil constitutionnel, en date du 10 février 2017, laquelle a expressément indiqué qu'une telle incrimination n'apparaissait pas nécessaire, dans son principe même, au sein d'une société démocratique ;

- En ce qu'il incrimine et punit la consultation habituelle sans définir les critères permettant de qualifier une consultation d'habituelle, prévoit une exception de motif légitime non limitative et n'apportent aucune définition de la notion de terrorisme et de manifestation à une idéologie ;

- En ce qu'il atteint à la liberté de communication et d'opinion de tout citoyen en punissant d'une peine privative de liberté la seule consultation de messages incitant au terrorisme alors que la personne concernée n'aurait commis ou tenté de commettre aucun acte pouvant laisser présumer qu'elle aurait cédé à cette incitation ou serait susceptible d'y céder, quand bien même cette dernière aurait manifesté son adhésion à l'idéologie véhiculée par ce service ;

- En ce qu'il crée une rupture d'égalité entre les personnes ayant accès à des tels messages, images ou représentations par un service de communication en ligne et celles y ayant accès par d'autres moyens et supports qu'un service de communication en ligne ;

- En ce qu'il crée une rupture d'égalité entre les citoyens souhaitant bénéficier d'un accès à de tels services et ceux excipant d'un motif légitime ou autorisés expressément par la Loi ;

- En ce qu'il punit de deux années d'emprisonnement et de 30 000 euros d'amende la seule consultation, même habituelle, d'un service de communication en ligne ;

---

14. Rapport n°4466 (AN) et n°399 (Sénat) de MM. Goasdoué et Grosdidier au nom de la commission mixte paritaire.
15. Cass. crim., 4 octobre 2017, *David X.*, n° 2518.

- En ce qu'il institue une présomption de mauvaise foi déduite de la seule consultation habituelle de ces services de communication en ligne.

La Cour de cassation estime légitime que le Conseil constitutionnel examine à nouveau l'article, remanié après sa précédente QPC du 10 février 2017, en relevant qu'une incertitude est susceptible de peser sur la notion de motif légitime rendant la consultation licite dès lors qu'elle n'est définie que par des exemples ; qu'il en est de même de la référence nécessaire à la manifestation de l'adhésion à l'idéologie exprimée sur le service concerné par l'auteur de la consultation.

Pour François Sureau « *avec ce délit ressuscité, on se trouve confronté à une forme d'acharnement parlementaire qui confine à l'obstination déraisonnable, pour emprunter au champ lexical de la fin de vie*[16] ».

Le 15 décembre 2017, la sanction tombe à nouveau : l'article 421-2-5-2 du code pénal, dans sa rédaction issue de la loi du 28 février 2017, est déclaré contraire à la Constitution.

Le Conseil s'appuie d'abord, comme il l'avait fait lors de la précédente censure, sur l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789, selon lequel *« La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi ».* Les Sages considèrent « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services* ». Ce même considérant avait été énoncé par le Conseil dans sa décision QPC du 10 février 2017, reprenant la formule énoncée dans sa décision du 10 juin 2009[17] à propos de la loi HADOPI I. Cette liberté comprend, rappelons-le, la liberté d'émettre ses opinions sur internet et celle aussi de recevoir l'information.

En vertu de l'article 34 de la Constitution, le législateur peut édicter des règles pour lutter contre l'incitation et la provocation au terrorisme sur les services de communication au public en ligne. Cette lutte participe, en effet, de l'objectif de sauvegarde de l'ordre public et de prévention des infractions qui a une valeur constitutionnelle. Mais ces règles doivent être conciliées avec l'exercice du droit de libre communication et de la liberté de parler, écrire et imprimer. Le Conseil ne fait que rappeler ici sa jurisprudence constante en matière d'ordre public.

---

16. François Sureau, avocat aux Conseils, plaidoirie du 4 décembre 2017 devant le Conseil constitutionnel.
17. Cons. const., déc. n°2009-577 DC du 3 mars 2009.

Les atteintes portées à l'exercice de cette liberté doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi. C'est sur cette trilogie que s'appuie à nouveau le Conseil pour censurer l'article.

Pour réfuter la nécessité, il dresse l'inventaire de toutes les possibilités offertes par le droit existant, tant en ce qui concerne les articles répressifs que les techniques d'enquête à la disposition des enquêteurs. Comme si l'énumération de la précédente QPC ne suffisait pas à éclairer la législateur, les Sages se livrent à un rappel du droit existant qui a la forme d'un corrigé type au profit d'un étudiant.

S'agissant des incriminations, l'article 421-2-1 du code pénal réprime 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 acte de terrorisme. L'article 421-2-4 du même code sanctionne 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 à une entente, prévus à l'article 421-2-1 ou qu'elle commette un acte de terrorisme. L'article 421-2-5 sanctionne le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes. L'article 421-2-5-1 réprime le fait d'extraire, de reproduire et de transmettre intentionnellement des données faisant l'apologie publique d'actes de terrorisme ou provoquant directement à ces actes afin d'entraver, en connaissance de cause, l'efficacité des procédures administratives de retrait, de blocage ou de déréférencement. Enfin, l'article 421-2-6 réprime le fait de préparer la commission d'un acte de terrorisme dès lors que cette préparation est intentionnellement en relation avec une entreprise individuelle ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur et qu'elle est caractérisée par le fait de détenir, de se procurer ou de fabriquer des objets ou des substances de nature à créer un danger pour autrui ainsi que par d'autres agissements tels que la consultation habituelle d'un ou de plusieurs services de communication au public en ligne provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie.

En ce qui concerne les techniques d'enquête - c'est-à-dire des investigations très intrusives dans la vie privée et placées sous le contrôle du juge des libertés et de la détention ou du juge d'instruction - le Conseil constitutionnel en dresse l'inventaire : interceptions de correspondances émises par voie de communication électronique, recueil des données techniques de connexion, sonorisation, fixation d'images et captation de données informatiques. Le Conseil souligne par ailleurs que, sauf pour les faits d'apologie du terrorisme et de provocation (article 421-2-5 du code pénal), des dispositions procédurales spécifiques prévues en matière de garde à vue et de perquisitions sont applicables.

On imagine, devant une telle énumération, que les Sages vont écarter la nécessité de l'incrimination contestée.

Mais, pour mieux charpenter leur démonstration, ils rappellent aussi que le législateur a conféré à l'autorité administrative de nombreux pouvoirs afin de prévenir la commission d'actes de terrorisme. Ainsi, pour satisfaire cette finalité, la loi du 24 juillet 2015 autorise les services de renseignement à employer des techniques de renseignement, mentionnées au titre V du livre VIII du code de la sécurité intérieure. Des procédures de retrait, de blocage et de déréférencement des sites de propagande terroriste sont prévues par le code de procédure pénale (art.706-23 sur référé ou requête du juge judiciaire) ou en vertu des dispositions de l'article 6-1 de la loi du 21 juin 2004 (loi pour la confiance dans l'économie numérique), telles qu'elles résultent de la loi du 13 novembre 2014 relative au terrorisme. Le Conseil constitutionnel mentionne également les dernières dispositions offertes par la loi du 30 octobre 2017 autorisant notamment les visites administratives.

Ces derniers éléments donneront des arguments à ceux qui, non sans raison, observent depuis quelques années un déplacement du centre de gravité de la matière pénale vers la police administrative.

Ainsi la décision du Conseil, pour contester la nécessité de l'article 421-2-5-2, considère que « *les autorités administrative et judiciaire disposent, indépendamment de l'article contesté, de nombreuses prérogatives, non seulement pour contrôler les services de communication au public en ligne provoquant au terrorisme ou en faisant l'apologie et réprimer leurs auteurs, mais aussi pour surveiller une personne consultant ces services et pour l'interpeller et la sanctionner lorsque cette consultation s'accompagne d'un comportement révélant une intention terroriste, avant même que ce projet soit entré dans sa phase d'exécution* ».

S'agissant des exigences d'adaptation et de proportionnalité requises en matière d'atteinte à la liberté de communication, espérant écarter les critiques objet de la QPC de février 2017, le législateur avait ajouté la manifestation de l'adhésion à l'idéologie exprimée sur ces services. Mais, pour le Conseil constitutionnel, cette consultation et cette manifestation ne sont pas susceptibles d'établir à elles seules l'existence d'une volonté de commettre des actes terroristes. L'exclusion de responsabilité pénale pour « motif légitime », alors que l'intention terroriste n'a pas été retenue comme élément constitutif de l'infraction, fait peser une incertitude sur la licéité de la consultation de certains services de communication au public en ligne et, en conséquence, de l'usage d'internet pour rechercher des informations.

Il résulte de tout ce qui précède que les dispositions contestées portent une atteinte à l'exercice de la liberté de communication qui n'est pas nécessaire, adaptée et proportionnée.

La censure du Conseil constitutionnel peut se résumer ainsi : vous avez les moyens juridiques et techniques de prévenir et de réprimer les infractions de contenus. N'en rajoutez pas ! Si l'on veut empêcher la consultation habituelle, il suffit de poursuivre ceux qui créent les sites, de responsabiliser les diffuseurs.

C'est vers cette nouvelle forme d'action que s'orientent désormais les pouvoirs publics en coopération avec les acteurs du web, dont les réseaux sociaux.

III. L'action sur les contenus avec le concours des acteurs du web

Avant la double sanction du Conseil constitutionnel, la loi avait donné aux pouvoirs publics la possibilité d'agir par des procédures judiciaires ou administratives de retrait, de blocage ou de déréférencement des sites incriminés (**A**). Depuis les attentats de 2015, une coopération se dessine avec les réseaux sociaux, soit à l'échelon national, soit à l'échelon européen ou international (**B**).

A. Les mesures de retrait, de blocage ou de déréférencement des contenus

Les contenus à caractère terroriste (et pédopornographique) peuvent, outre les poursuites pénales, entraîner des mesures de retrait ou de blocage prises par l'autorité judiciaire (**1**) ou au titre de la police administrative (**2**). Ces mesures s'adressent à des acteurs qui ont été définis par la loi pour la confiance dans l'économie numérique : les fournisseurs d'accès à internet (FAI), les hébergeurs et les éditeurs.

1. L'intervention judiciaire relative à un contenu terroriste

Plusieurs textes de lois permettent à l'autorité judiciaire d'agir face à un contenu illicite.

Selon le paragraphe 8 du I de l'article 6 de la loi pour la confiance dans l'économie numérique, l'autorité judiciaire peut 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* ». Le référé au civil s'appuie sur l'article 809 du code de procédure civile. L'article 50-1 de loi du 29 juillet 1881 relative à la liberté de la presse, créé par la loi du 5 mars 2007 relative à la prévention de la délinquance, dispose que, lorsque certains contenus constituent un trouble manifestement illicite, « *l'arrêt du service peut être prononcé par le juge de référés, à la demande du ministère public et de toute personne physique ou morale ayant intérêt à agir* ». Du fait du transfert dans le code pénal des infractions de provocation et d'apologie du terrorisme, la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme introduit une disposition similaire dans le code de procédure pénale (article 706-23). L'article 50-1 s'applique toujours aux autres contenus illicites.

Le juge judiciaire peut également intervenir pour condamner l'auteur d'une entrave aux mesures d'arrêt, de blocage ou de retrait des sites à caractère terroriste. La loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale crée, en effet, une nouvelle infraction qui réprime le fait d'extraire, de reproduire et de transmettre intentionnellement des données faisant l'apologie publique d'actes de terrorisme ou provoquant directement à ces actes en vue d'entraver les mesures d'arrêt d'un service de communication en ligne par voie judiciaire ou les retraits ou blocages demandés par l'autorité administrative en vertu de l'article 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

On notera cependant que la jurisprudence judiciaire est, dans les deux cas, plutôt pauvre en la matière. C'est la preuve d'un recours privilégié aux mesures administratives.

2. Les mesures prises au titre de la police administrative

Parmi les principales mesures de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, l'article 12 est celui qui suscite le plus de critiques. Il modifie, en effet, l'article 6 de la loi sur la confiance dans l'économie numérique en transférant dans un nouvel article 6-1 les modalités qui s'appliquent aux contenus provoquant au terrorisme ou faisant leur apologie ou le blocage administratif des sites qui y donnent accès.

Les mesures de blocage ou de retraits de contenus constituent une nouvelle forme de police administrative spéciale, dont le contentieux relève du juge administratif.

Considérant que le juge judiciaire est le gardien des libertés, certains parlementaires et la plupart des acteurs d'internet (Conseil National du Numérique en particulier) voudraient lui donner le monopole de toute intervention relative aux contenus, eu égard à l'atteinte portée à la liberté d'expression par une mesure de retrait ou de blocage. Ils s'opposent donc au développement d'une police administrative des contenus. Ces opposants se sont fait notamment entendre lors des débats relatifs à la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

La procédure issue de la loi du 13 novembre 2014 est identique à celle prévue pour les sites pédopornographiques. Elle concerne le retrait des sites et, à défaut, leur blocage. Elle peut également porter sur le déréférencement des sites illicites.

Les décrets du 5 février 2015[18] et du 4 mars 2015[19] étaient attendus ! Relatifs au retrait, au blocage ou au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique, ils sont publiés dans un délai à la fois très court et très long, selon que l'on considère le terrorisme ou la pédopornographie. Dans le second cas, en effet, le texte source est la loi du 14 mars 2011 modifiant l'article 6 de loi pour la confiance dans l'économie numérique. Le décret d'application tardait à venir. Le gouvernement, lors des débats sur la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, avait annoncé la publication d'un texte commun. Les attentats qui ont frappé la France au début de 2015 expliquent sans doute la célérité avec laquelle les décrets ont été publiés.

Les attentats du 13 novembre 2015 ont également mis en sourdine les critiques émises lors du vote de la loi. Faute d'une saisine directe du Conseil constitutionnel, l'Association des services internet communautaires (ASIC[20]) souhaitait que le Conseil d'État transmette une question prioritaire de constitutionnalité lors de l'examen des décrets d'application[21]. Tel n'a pas été le cas. Les deux décrets ont fait, sans succès, l'objet d'un recours pour excès de pouvoir devant le Conseil d'État[22,] formé par l'association *French Data Network*, *La Quadrature du Net* et la *Fédération des fournisseurs d'accès à l'internet associatifs*.

a. Le retrait et le blocage des sites

L'autorité administrative mentionnée à l'article 6-1 de la loi du 21 juin 2004 est, selon l'article 1er du décret du 5 février 2015, l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui agit par des agents spécialement habilités. L'office applique un principe de subsidiarité : il s'adresse d'abord aux éditeurs et hébergeurs afin qu'ils retirent les contenus dans un délai de 24 heures. En cas d'échec, ou directement si l'éditeur ou l'hébergeur ne

18. Décret n° 2015-125 du 5 février 2015 *relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique* (*JORF*, 6 février 2015, p. 1811).
19. Décret n° 2015-253 du 4 mars 2015 *relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique* (*JORF*, 5 mars 2015, p. 4168).
20. L'ASIC regroupe notamment *Google*, *Facebook*, *Microsoft*, *eBay*, *Yahoo*, *Dailymotion*, *Deezer*, *Spotify*, *Airbnb*, *AOL*, *Skyrock*, *PriceMinister*, *Skype*.
21. Le Conseil constitutionnel (déc. n° 2011-625 DC du 10 mars 2011) a rappelé que le blocage d'un site internet constitue une atteinte grave à la liberté d'expression et de communication, tout en déclarant conforme à la Constitution les blocages des sites pédophiles.
22. CE, 2ème/7ème SSR, 15 février 2016, *Association French Data Network et autres*, n° 389140.

peuvent être identifiés[23] (dans la pratique, ils le sont très rarement, car résidant à l'étranger), les fournisseurs d'accès sont invités à bloquer l'accès au(x) site(s) incriminé(s). L'OCLCTIC met à la disposition de la personnalité qualifiée désignée au sein de la CNIL les demandes de retrait adressées aux hébergeurs et aux éditeurs ainsi que les éléments établissant la méconnaissance par les contenus des services de communication au public en ligne des articles 227-23 et 421-2-5 du code pénal. Lui sont transmis des documents précis (captures d'écran, extraits de textes, etc.) qui lui évitent de rechercher elle-même les éléments constitutifs en visionnant l'ensemble du site concerné.

La liste des adresses électroniques[24] des services de communication au public en ligne est adressée aux FAI selon un mode de transmission sécurisé, qui en garantit la confidentialité et l'intégrité. L'article 2 du décret précise que les utilisateurs des services de communication au public en ligne, auxquels l'accès est empêché, sont dirigés vers une page d'information du ministère de l'intérieur, indiquant pour chacun des deux cas de blocage les motifs de la mesure de protection et les voies de recours. Les agents des services de l'État compétents en matière de prévention et de répression du terrorisme ou de lutte contre la pédopornographie ainsi que la personnalité qualifiée conservent un accès aux adresses électroniques des services de communication au public en ligne auxquels l'accès est empêché.

b. Le déréférencement de sites illicites

L'autorité administrative a également le pouvoir de s'adresser directement aux moteurs de recherche ou aux annuaires pour qu'ils cessent de référencer les sites illicites. Cette dernière mesure est déjà appliquée en vertu de l'article 61 la loi n°2010-476 du 12 mai 2010, relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne. Mais dans ce cas, l'intervention du juge judiciaire est nécessaire. Le décret n° 2015-253 du 4 mars 2015 précité s'appuie sur l'article 6-1 de la loi n°2004-575 du 21 juin 2004 (LCEN) modifié par l'article 12 de la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la loi sur le terrorisme.

L'OCLCTIC peut demander aux exploitants de moteurs de recherche ou d'annuaires de déréférencer les adresses qui contreviennent aux dispositions des articles 227-3 (pédopornographie) et 421-2-5 (terrorisme) du code pénal. Cette démarche est accompagnée d'une transmission sans délai à la personnalité désignée en son sein par la CNIL qui peut exercer un contrôle. La liste doit être actualisée tous les trimestres. Le déréférencement doit intervenir dans les quarante-huit heures suivant la notification. Il en est de

23. Par exemple, si l'éditeur ne fournit pas les informations prévues par l'article 6-III de la LCEN (identité, domicile, raison sociale).
24. Ces adresses comportent soit un nom de domaine (DNS), soit un nom d'hôte caractérisé par un nom de domaine précédé d'un nom de serveur.

même pour le rétablissement du référencement, lorsque les sites ne présentent plus de caractère illicite.

c. Un débat révélateur de clivages qui transcendent les courants politiques

Deux questions sont soulevées : peut-on bloquer, retirer ou déréférencer des contenus sans porter atteinte à la liberté d'expression ? Dans l'affirmative, quel est le juge compétent ?

L'opposition au retrait ou au blocage par voie administrative s'exprime aussi bien dans la majorité que dans l'opposition parlementaire, mais elle est minoritaire. Elle est soutenue notamment par l'ASIC et la Commission nationale consultative des droits de l'homme (CNCDH). Le gouvernement français et ceux qui le soutiennent lors de l'élaboration de la loi du 13 novembre 2014 ne sous-estiment pas l'efficacité limitée du blocage des sites, mais ils considèrent qu'il n'est pas acceptable dans une société libre et démocratique que des contenus mettent en scène des personnes décapitées, violées, crucifiées, brûlées vives. Ils sont soutenus par Maître Jakubowicz, président de la LICRA, pour qui « *les fournisseurs d'accès doivent sortir d'une certaine hypocrisie et épauler les avancées permettant de lutter contre les atteintes à la dignité, voire à la vie humaine* »[25].

S'agissant des aspects juridiques, les opposants considèrent que le retrait ou le blocage est une atteinte telle à la liberté d'expression que celle-ci requiert l'intervention du juge judiciaire. La Commission de réflexion sur le droit et les libertés à l'âge du numérique[26] estime, dans sa recommandation de juillet 2014, que « *le préalable d'une décision judiciaire apparaît comme un principe essentiel, lorsqu'est envisagé le blocage de l'accès à des contenus illicites sur des réseaux numériques* ». Le Conseil National du Numérique, dans son avis rendu le 15 juillet 2014[27], a une position similaire : sans s'opposer au blocage ou au filtrage de contenus quand ils sont illicites, il préconise 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 des contenus sur internet. Le rapport de Marc Robert est plus partagé : il recommande que la décision de blocage d'un site vienne du juge judiciaire (juge civil ou juge des libertés et de la détention) saisi par l'administration, compte tenu des effets sur les libertés individuelles, mais qu'une exception doit être faite pour la pédopornographie,

25. *AFP*, 10 juillet 2014 (à propos du projet de loi relatif au terrorisme).
26. Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, co-présidée par le député (PS) Christian Paul et l'avocate Christiane Féral-Schuhl et composée de 13 députés et de 13 personnalités qualifiées.
27. Avis n°2014-3 du 15 juillet 2014 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme.

cette infraction étant avérée par nature et le dispositif de blocage administratif sans intervention judiciaire ayant été validé par le Conseil constitutionnel[28].

Du point de vue de l'efficacité, selon les détracteurs du texte, de nombreux sites incriminés (90 à 95%) sont hébergés au Canada ou aux États-Unis, ce qui rend la procédure de retrait quasi inopérante. 80% des contenus illicites sont véhiculés par *Facebook*, *Twitter* ou *Youtube*. Les blocages par inspections de contenus (*Deep Packet Inspection*- DPI) sont attentatoires aux libertés, car ils consistent à inspecter l'ensemble des échanges. Les blocages par adresse IP, par nom de domaine ou URL sont les plus aisés à mettre en place mais ils conduisent à des « surblocages » ou sont inefficaces, car contournables. L'abonnement à un réseau virtuel privé (VPN), qui permet de surfer sur internet à partir du pays de son choix, permet, en effet, de ne pas subir un blocage limité aux internautes français. Le logiciel TOR (*The Onion Router*) offre également une solution qui garantit l'anonymat.

L'efficacité du dispositif de blocage serait très réduite selon les détracteurs de la loi. Le recours au chiffrement par les terroristes viendrait compliquer la tâche des services spécialisés. « *On ne coupe pas le téléphone de celui que l'on veut écouter* », selon certains de leurs membres qui craignent une perte d'efficacité des enquêtes sur les milieux terroristes. Ainsi le juge anti-terroriste, Marc Trévidic considère que *« toutes les personnes arrêtées depuis 2007 l'ont été grâce aux imprudences commises sur internet, à la communication électronique. Si nous les empêchons de surfer, nous aurons plus de mal à détecter leurs agissements. Les sites pratiquant le prosélytisme peuvent toucher un large public, on peut donc souhaiter limiter cette propagande. Cependant la part la plus dangereuse de leurs activités se déroule sur messageries privées et c'est parce que nous visitons ces dernières que nous savons ce qui se passe* »[29].

Le retrait et le blocage, certes contournables par les plus experts, doivent prévenir l'accès involontaire du plus grand nombre. Le blocage, jugé par certains attentatoire à la liberté d'expression, n'est que l'ultime recours, le retrait étant la règle qui témoigne de l'esprit de responsabilité des hébergeurs, tel qu'il s'est d'ailleurs manifesté après les attentats du 7 janvier 2015.

Sur le recours à une procédure de police administrative, le rapporteur de la loi à l'Assemblée nationale, Sébastien Pietrasanta, considère que « *ce que l'autorité administrative peut faire dans la sphère réelle pour protéger l'ordre public, elle doit également pouvoir le faire dans la sphère numérique* »[30]. Bernard Cazeneuve renchérit : « *Si des appels se produisaient sur un autre espace public, un autre espace de liberté, et non sur la Toile, l'espace numérique, je suis convaincu que tous ceux qui siègent dans l'hémicycle me demanderaient les raisons pour lesquelles je ne fais pas cesser le trouble à*

28. Marc Robert, « *Protéger les internautes* » – Rapport sur la cybercriminalité, février 2014.
29. Marc Trévidic, juge anti-terroriste, *in* David Assouline, Compte-rendu sur « Le contrôle et l'évaluation des dispositifs législatifs relatifs à la sécurité intérieure et à la lutte contre le terrorisme », Sénat, octobre 2012, p. 37.
30. *JOAN*, déb., 1ère séance, 15 septembre 2014, p. 6316.

l'ordre public, et ils auraient toute légitimité à la faire. Mais dès lors qu'il s'agirait d'internet, il ne serait plus possible de procéder ainsi parce que la prévention du risque et la mesure de police en vue de rétablir ou d'assurer l'ordre public serait liberticides ! »[31].

Quant à l'intervention du juge judiciaire, par préférence au juge administratif, Jean Jacques Hyest, alors rapporteur de la loi au Sénat, déclare : « *Certains voudraient que la justice judiciaire s'occupe de tout. Mais le rôle de la justice judiciaire, c'est de réprimer ! Et si l'on commence à tout mélanger, à faire intervenir le juge judiciaire dans les affaires de police administrative, on détruira en partie un édifice auquel beaucoup d'entre nous sont attachés* »[32].

Pour éclairer le débat, on peut émettre deux observations : si l'infraction est constituée, rien n'empêche le juge judiciaire de se saisir, dès lors qu'il est territorialement compétent[33] et de procéder lui-même aux démarches aboutissant au retrait ou au blocage. La crainte de sa lenteur semble motiver le choix du législateur. Il appartient donc au juge judiciaire de faire preuve de réactivité. S'agissant de la technique du blocage, comme le souligne le rapport de Marc Robert, « *elle n'est pas la panacée – mais celle-ci n'existe que rarement dans le domaine de la lutte contre la cybercriminalité – elle constitue un outil, parmi d'autres, dont on aurait tort de se priver à condition de le cantonner strictement* ».

C'est donc dans un contexte plutôt apaisé que l'autorité qualifiée, Alexandre Linden, conseiller honoraire près la Cour de cassation, a rendu ses deux premiers rapports, selon les modalités prévues par l'article 6-1 de la loi pour la confiance dans l'économie numérique.

d. Les premiers bilans

Dans son premier rapport, Alexandre Linden évoque 25 séances de vérifications tenues entre mars 2015 et février 2016. Ces séances portent également sur les « contre-vérifications », c'est-à-dire sur l'obligation qui pèse sur l'OCLCTIC de vérifier que les contenus sont toujours illicites.

Période février 2015/ mars 2016	Demandes de retrait	Retraits effectués	Demandes de blocage	Demandes de déréférencement
Terrorisme	1286	1080	68	386
Pédopornographie	153	99	244	469
Total	1439	1179	312	855

31. *JO*, Sénat, déb., séance du 15 octobre 2014, p. 7045.
32. *Id.*, p. 7049.
33. Les contenus incriminés doivent être accessibles depuis le territoire français.

Dans son deuxième rapport du 3 mai 2017, l'autorité qualifiée souligne la forte croissance du nombre de vérifications opérées (près de 78% par rapport à la période précédente). Le tableau ci-dessous en témoigne.

	Demandes de retrait	Retraits effectués	Demandes de blocage	Demandes de déréférencement
Totaux (2016-2017)	2 561	2 305	874	2077
Totaux (2015-2016)	1 439	1 179	312	855
Augmentation de l'activité de contrôle par rapport à la période précédente	+77,97%	+95,5%	+180,12%	+142,9%

Source Rapport Linden 2017

Au total, 5512 demandes ont été adressées par l'OCLCTIC sur la période. Ont été examinées :

- 874 demandes de blocage de sites ;

- 2 561 demandes de retrait de contenus ;

- 2 077 demandes de déréférencement d'adresses électroniques provoquant à des actes de terrorisme ou en faisant l'apologie, ou à caractère pédopornographique.

Les contenus à caractère terroriste représentent 60% des contrôles opérés.

Le rapport précise que 712 d'entre elles ont fait l'objet de demandes de complément liées à l'insuffisance de justification. 10 recommandations ont été notifiées à l'OCLCTIC dont 4 résultant d'un désaccord entre l'OCLCTIC et la personnalité qualifiée, selon qui les éléments de contexte de diffusion ne permettaient pas d'établir le caractère illicite du contenu.

Comme en 2016, Alexandre Linden n'a constaté aucun cas de surblocage, risque mis en avant par les opposants à la loi lors de son l'élaboration.

Si le bilan est globalement rassurant, il met en évidence les faibles moyens de l'autorité qualifiée au regard d'une mission dont la charge est croissante.

Les chiffres présentés, quelle que soit leur progression, restent très faibles au regard de l'ampleur des phénomènes incriminés. En près deux années (2015-2017), Twitter annonce avoir supprimé sur l'ensemble de la planète 900.000 comptes faisant l'apologie du terrorisme, dont 300.000 pendant les six premiers mois de l'année 2017. *Facebook* emploie plus de 150 personnes pour lutter contre les contenus illicites. Ces statistiques expliquent sans doute pourquoi Daech a menacé Mark Zuckerberg et Jack Dorsey, respectivement patrons de *Facebook* et de *Twitter*, pourtant souvent accusés de ne pas assez lutter contre le cyberterrorisme.

B. La régulation par les réseaux sociaux : « je t'aime, moi non plus ! »

La France choisit le dialogue avec les réseaux sociaux après l'attentat ayant visé *Charlie Hebdo*. Au printemps 2015, Bernard Cazeneuve, alors ministre de l'intérieur, est allé à leur rencontre dans la *Silicon Valley*. Cette démarche n'est pas isolée.

Suite au conseil Justice Affaires Intérieures extraordinaire du 24 mars 2016, faisant suite aux attentats de Bruxelles, la Commission européenne établit, en mai 2016, un code de bonne conduite avec *Facebook*, *Twitter*, *Youtube* et *Microsoft* pour empêcher la propagation de discours haineux illégaux en ligne. En particulier, « *les entreprises des technologies de l'information doivent mettre en place des procédures claires et efficaces d'examen des signalements de discours haineux illégaux diffusés via leurs services de manière à pouvoir retirer les contenus concernés ou à en bloquer l'accès. Elles établissent des règles ou des lignes directrices internes précisant qu'elles interdisent la promotion de l'incitation à la violence et aux comportements haineux* ».

Lors de leur rencontre, le 13 juin 2017, Theresa May et Emmanuel Macron ont annoncé la mise au point d'un plan d'action conjoint pour lutter contre l'emploi d'internet à des fins terroristes. Il est demandé aux entreprises concernées d'agir en priorité dans trois domaines :

- le retrait des contenus terroristes dans un délai d'une à deux heures suivant leur publication ;

- la lutte contre l'enfermement algorithmique ;

- le soutien aux entreprises de taille plus modeste pour les aider à détecter ces contenus et à prévenir leur réapparition.

Le lendemain, *Facebook* présente des mesures.

Plus répressive, tout en étant ouverte au dialogue, l'Allemagne veut montrer sa détermination en promulguant une loi[34] obligeant les réseaux sociaux à supprimer les messages haineux dans les 24 heures et de ne pas republier un contenu déjà supprimé, sous peine d'amende pouvant atteindre cinquante millions d'euros.

Les réseaux sociaux ne sont pas insensibles aux contenus dont ils favorisent la diffusion, pour le meilleur comme pour le pire, mais ils sont souvent accusés de laxisme. Comprenant sans doute que la pression internationale augmentait, *Facebook*, *Twitter*, *Youtube* et *Microsoft* s'unissent au sein du *Global Internet Forum to Counter Terrorism* (GIFCT) pour détecter les contenus terroristes. Une base de données partagées permet d'identifier les contenus déjà supprimés, tandis que l'intelligence artificielle

34. *Netzwerkfdurchsetzungsgesetz* (NetzDG) approuvée en Conseil des ministres fédéraux le 5 avril 2017 et entrée en vigueur le 1er octobre 2017. Le texte suscite de nombreuses critiques venant notamment de ceux qui craignent un excès de zèle au regard des sanctions encourues.

identifie les nouveaux avec l'aide de personnes qualifiées, car l'apport de l'humain est ici indispensable pour faire la distinction entre la propagande et la liberté d'expression ou d'information.

Le 28 septembre 2017, faisant suite à la lettre d'intention du 13 septembre 2017 que le président de la Commission européenne a adressée au président du Parlement européen et au président du Conseil de l'Union européenne, la Commission présente des « *orientations et des principes afin que les plateformes en ligne renforcent la prévention, la détection et la suppression proactives des contenus illicites en ligne* ».

La communication prévoit un ensemble de dispositions accentuant leur coopération avec les autorités nationales, les États membres et les autres acteurs concernés.

Elle vise à faciliter et à accélérer la mise en œuvre de bonnes pratiques pour interdire, détecter, supprimer et bloquer l'accès au contenu illicite de façon à garantir le retrait effectif de celui-ci, une transparence accrue et la protection des droits fondamentaux en ligne. Elle vise aussi à apporter aux plateformes des précisions sur leurs responsabilités lorsqu'elles prennent des mesures proactives (dites de « Bon Samaritain ») pour détecter, supprimer ou bloquer l'accès au contenu illicite.

Quelques jours plus tard, en octobre, le G7 et les majors d'internet (*Google*, *Facebook*, *Twitter*) se réunissent sur l'île italienne d'Ischia pour sceller un accord ayant pour objectif de supprimer les contenus à caractère terroriste dans les deux heures suivant leur mise en ligne. Cet accord supposait que les États-Unis fassent preuve de plus de discernement dans l'application du Premier amendement de la Constitution américaine qui privilégie la liberté d'expression. Les Européens ont obtenu gain de cause.

La responsabilisation des réseaux sociaux est donc la voie privilégiée. Le 13 novembre 2017, interrogé sur le harcèlement et les messages de haine, Mounir Mahjoubi, secrétaire d'État au numérique, souhaite agir grâce et avec les opérateurs des grands réseaux « *parce qu'on saura leur rappeler leur responsabilité. Les plateformes* – poursuit-il – *ont cette capacité à réagir dans l'heure, dans les 24 heures. Elles sont prêtes à se mobiliser pour un téton apparent en quelques minutes et le faire supprimer, et moins sur un message de haine. Donc on leur dit :si vous êtes capables de vous mobiliser sur un téton, mobilisez-vous sur les messages de haine* »[35].

Au même moment, *Youtube* supprime des vidéos d'Anwar Al-Awakli, un des plus grands recruteurs djihadistes tué par un drone. Grâce à un algorithme, plus de 50.000 vidéos sont ainsi supprimées.

35. Interview de M. Mounir Mahjoubi, *Europe 1*, 13 novembre 2017. La référence au téton s'explique par la censure, début 2017, par *Facebook* de photos présentées par une tatoueuse britannique pour montrer comment procéder à une reconstruction mammaire après un cancer ou un accident. *Facebook* s'était excusé.

Le mardi 6 décembre 2017 se tient à Bruxelles le *Forum de l'Union européenne sur l'internet*[36], réunion au niveau ministériel. Les commissaires européens Dimitris Avramopoulos et Julian King accueillent les États membres, Europol, des experts de l'Union européenne et des entreprises majeures du secteur de l'internet, en vue de débattre des progrès accomplis dans la lutte contre les contenus à caractère terroriste en ligne et d'intensifier les futures actions de l'Union européenne dans ce domaine. Le Forum de l'Union européenne sur l'internet vise deux objectifs : réduire l'accessibilité des contenus à caractère terroriste en ligne et donner aux partenaires de la société civile les moyens d'accroître, sur l'internet, le volume de contre-discours efficaces.

La négociation « *ferme* » avec les réseaux sociaux semble être la stratégie arrêtée au plus haut niveau par le gouvernement français début octobre 2017. David Martinon, ambassadeur en charge des négociations relatives à l'espace numérique est le point de contact avec les GAFA, tandis que la Délégation ministérielle aux industries de sécurité et aux cybermenaces (DMISC) anime un groupe de travail commun.

Lors de la présentation de la stratégie internationale de la France pour le numérique, le 15 décembre 2017, Jean-Yves Le Drian précise la position du gouvernement français : « *La France considère, avec ses partenaires européens, que les entreprises du secteur numérique doivent assumer leurs responsabilités dans la lutte contre le terrorisme et la criminalité en ligne. Dans ce domaine, l'efficacité de notre action suppose de faire preuve d'innovation diplomatique. La France entend donc agir avec les grands acteurs de l'internet (Facebook, Microsoft, Twitter et YouTube notamment) puisque ce sont leurs plateformes qui servent de support à ce champ de bataille d'un genre nouveau. C'est de cette manière que nous pourrons lutter efficacement contre la propagande, le recrutement, la planification opérationnelle à des fins terroristes, ainsi que la dissémination en ligne des discours et des images de haine* ».

Dialoguer est sans doute la voie la plus efficace, mais il ne faut pas abandonner aux réseaux sociaux la responsabilité du contrôle des contenus. Ils ne peuvent être érigés en juges et encore moins en censeurs des contenus, car ils font parfois preuve d'un certain manque de discernement[37]. Les mots, les photos, les paroles, peuvent avoir des significations différentes selon les pays, les circonstances. Quelle que soit la qualité des algorithmes mis en œuvre par les réseaux, il n'est pas envisageable de leur abandonner la décision, même si *Facebook*, *Twitter* ou *Youtube* annoncent un renforcement des équipes en charge du contrôle afin de laisser l'humain le soin de décider en dernier ressort.

---

36. Ce Forum a été lancé en décembre 2015 par M. Dimitris Avramopoulos, Commissaire pour la migration, les affaires intérieures et la citoyenneté, afin de mettre un terme à l'utilisation abusive de l'internet par des groupes terroristes internationaux

37. Par exemple, le tableau « Origine du monde » de Courbet censuré pour pornographie ou la « Petite sirène de Copenhague » considérée comme représentation pédophile…

Pour autant, les réseaux sociaux doivent s'engager davantage pour veiller sur les « *autoroutes de l'information* ». Il s'agit à n'en point douter d'une forme, même partielle, de délégation de service public, la sécurité des réseaux ne se limitant plus à leurs couches matérielles et logicielles.

Conclusion

Le terrorisme est doublement dangereux, par ses conséquences physiques et psychiques sur les personnes, mais aussi par son impact sur les institutions. Pour lutter contre ce fléau, les gouvernements sont tentés de renforcer leur arsenal législatif et les moyens des forces de sécurité. On ne peut leur reprocher de tout mettre en œuvre pour prévenir des comportements odieux, notamment grâce à l'action des services de renseignement et des services enquêteurs. Les « *notes blanches* » qui se succèdent sur les bureaux du gouvernement sont de nature à renforcer la conviction des décideurs politiques. Pour autant, le risque est grand de porter atteinte aux libertés, par sédimentation de lois successives qui s'appuient sur des considérations légitimes, mais peuvent avoir un impact sur les démocraties. C'est sans doute l'un des objectifs des terroristes pour placer leurs adversaires devant leurs contradictions. La lutte contre le terrorisme ne peut se satisfaire d'une réponse réduite au droit à qui l'on demanderait de réguler ce qui relève de la responsabilité individuelle et collective. Avec la couche cognitive du web se démultiplie la puissance du verbe, du discours. En 1970, Michel Foucault s'exprimait en ces termes dans sa leçon introductive au Collège de France : « *je suppose que dans toute société la production du discours est à la fois contrôlée, sélectionnée, organisée et redistribuée par un certain nombre de procédures qui ont pour rôle d'en conjurer les pouvoirs et les dangers, d'en maîtriser l'événement aléatoire, d'en esquiver la lourde, la redoutable matérialité* ».

Depuis, le web, les réseaux sociaux ont profondément modifié nos modes d'expression. La pensée foucaldienne peut-elle encore expliquer le discours, tant la production, la sélection, la redistribution du discours échappe aujourd'hui aux procédures traditionnelles ? Dans une interview au *Guardian*[38], le 12 mars 2017, Sir Tim Berners Lee s'inquiète de l'évolution du web qu'il faut, selon lui, sauver, notamment parce qu'il est utilisé pour des actions de désinformation qui peuvent avoir des fins politiques ou financières. Les « *autoroutes de l'information* » peuvent se transformer en « *autoroutes de la désinformation* ». Le terrorisme via internet est sans doute l'occasion de prendre conscience des dangers qui pèsent sur l'espace numérique. La réponse est sans doute plus philosophique et politique que juridique.

38. Tim Berners-Lee, « I invented the web. Here are three things we need to change to save it », *The Guardian,* 12 mars 2017.