



Conseil de  
l'Union européenne

Bruxelles, le 7 mars 2018  
(OR. en)

6717/18

CYBER 39  
TELECOM 51  
CT 31  
FREMP 22  
JAI 181  
AUDIO 10  
DROIPEN 26  
COHOM 34

#### NOTE DE TRANSMISSION

---

Origine:	Pour le secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, directeur
Date de réception:	7 mars 2018
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	C(2018) 1177 final
Objet:	RECOMMANDATION DE LA COMMISSION du 1.3.2018 sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne

---

Les délégations trouveront ci-joint le document C(2018) 1177 final.

---

p.j.: C(2018) 1177 final



Bruxelles, le 1.3.2018  
C(2018) 1177 final

**RECOMMANDATION DE LA COMMISSION**

**du 1.3.2018**

**sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en  
ligne**

## RECOMMANDATION DE LA COMMISSION

du 1.3.2018

### sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 292,

considérant ce qui suit:

- (1) L'internet et les prestataires de services internet contribuent de manière significative à l'innovation, à la croissance économique et à la création d'emplois dans l'Union. Nombre de ces prestataires de services jouent un rôle essentiel dans l'économie numérique en mettant en relation les entreprises et les citoyens et en facilitant le débat public et la diffusion et la réception d'informations factuelles, d'opinions et d'idées. Dans certains cas, cependant, des tiers utilisent de manière abusive les services fournis par ces prestataires pour mener des activités illicites en ligne, comme par exemple diffuser certaines informations relatives au terrorisme, du matériel pédopornographique ou des discours de haine illégaux ou commettre des infractions à la législation sur la protection des consommateurs, ce qui peut entamer la confiance de leurs utilisateurs et porter atteinte à leurs modèles économiques. Parfois, il est même possible que les prestataires concernés tirent certains avantages de ces activités, par exemple du fait de la mise à disposition de contenus protégés par le droit d'auteur sans le consentement des titulaires de droits.
- (2) La présence de contenus illicites en ligne entraîne d'importantes conséquences négatives pour les utilisateurs, pour d'autres citoyens et entreprises concernés et pour la société dans son ensemble. Compte tenu de leur rôle central et des moyens et capacités technologiques associés aux services qu'ils fournissent, les prestataires de services en ligne ont la responsabilité particulière, vis-à-vis de la société, de contribuer à la lutte contre les contenus illicites diffusés au moyen de leurs services.
- (3) Comme il est souvent essentiel d'agir rapidement pour retirer les contenus illicites ou en rendre l'accès impossible afin d'enrayer leur diffusion et de limiter le préjudice causé, ces responsabilités impliquent notamment que les prestataires de services en question devraient pouvoir prendre des décisions rapides quant aux éventuelles mesures à appliquer concernant les contenus illicites en ligne. Ils devraient également, dans le cadre de ces responsabilités, mettre en place des mesures de sauvegarde efficaces et adéquates, notamment pour garantir qu'ils agissent avec diligence et de manière proportionnée et pour éviter le retrait non intentionnel de contenus qui ne sont pas illicites.
- (4) De nombreux prestataires de services en ligne ont reconnu ces responsabilités et y ont donné suite. Au niveau collectif, d'importants progrès ont été accomplis grâce à des accords volontaires de diverses natures, notamment le forum de l'UE sur l'internet consacré aux contenus terroristes en ligne, le code de conduite visant à combattre les discours de haine illégaux en ligne et le protocole d'accord sur la vente de

contrefaçons. Toutefois, malgré cette mobilisation et les progrès réalisés, les contenus illicites en ligne restent un problème grave au sein de l'Union.

- (5) Préoccupé par une série d'attaques terroristes dans l'UE et la diffusion de propagande terroriste en ligne, le Conseil européen des 22 et 23 juin 2017 a déclaré qu'il «*attend des entreprises du secteur qu'elles [...] mettent au point de nouvelles technologies et de nouveaux outils en vue d'améliorer la détection automatique et la suppression des contenus qui incitent à la commission d'actes terroristes*». Le Parlement européen, dans sa résolution du 15 juin 2017, demandait instamment aux plateformes en ligne «*de renforcer leurs mesures de lutte contre les contenus en ligne illégaux et dangereux*». L'appel lancé aux entreprises pour qu'elles adoptent une approche plus proactive afin de protéger leurs utilisateurs des contenus à caractère terroriste a été réitéré par les ministres des États membres au sein du forum de l'UE sur l'internet. En ce qui concerne les droits de propriété intellectuelle, dans ses conclusions du 4 décembre 2014 sur le respect de ces droits, le Conseil a invité la Commission à se pencher sur le recours aux outils disponibles pour identifier les auteurs de violations des droits de propriété intellectuelle et sur le rôle que jouent les intermédiaires pour contribuer à la lutte contre de telles violations.
- (6) Le 28 septembre 2017, la Commission a adopté une communication contenant des orientations sur les responsabilités des prestataires de services en ligne en ce qui concerne les contenus illicites en ligne<sup>1</sup>. Dans cette communication, la Commission expliquait qu'elle allait déterminer si des mesures supplémentaires s'imposaient, notamment en assurant un suivi des progrès accomplis sur la base d'accords volontaires. La présente recommandation fait suite à cette communication, reflétant son niveau d'ambition et en assurant la mise en œuvre, tout en prenant dûment en compte les avancées importantes enregistrées grâce à ces accords volontaires et en s'appuyant sur celles-ci.
- (7) La présente recommandation reconnaît qu'il convient de prendre dûment en compte les particularités de la lutte contre différents types de contenus illicites en ligne et les réponses spécifiques qui pourraient s'avérer nécessaires, y compris des mesures législatives. Par exemple, reconnaissant la nécessité de telles mesures législatives spécifiques, la Commission a adopté, le 25 mai 2016, une proposition de modification de la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels, compte tenu de l'évolution des réalités du marché<sup>2</sup>. Le 14 septembre 2016, la Commission a également adopté une proposition de directive sur le droit d'auteur dans le marché unique numérique<sup>3</sup>, qui prévoit l'obligation pour certains prestataires de services de prendre, en coopération avec les titulaires de droits, des mesures destinées à assurer le bon fonctionnement des accords conclus avec les titulaires de droits en ce qui concerne l'utilisation de leurs œuvres ou autres objets protégés ou destinées à empêcher la mise à disposition, par leurs services, d'œuvres ou d'autres objets protégés identifiés par les titulaires de droits en coopération avec les prestataires de services. La présente recommandation n'affecte en rien ces mesures et propositions législatives.

---

<sup>1</sup> COM(2017) 555 final du 28 septembre 2017.

<sup>2</sup> COM(2016) 287 final du 25 mai 2016.

<sup>3</sup> COM(2016) 593 final du 14 septembre 2016.

- (8) La directive 2000/31/CE du Parlement européen et du Conseil<sup>4</sup> prévoit des dérogations en matière de responsabilité qui sont, sous réserve de certaines conditions, applicables à certains prestataires de services en ligne, y compris les prestataires de services d'«hébergement» au sens de son article 14. Pour bénéficier de cette dérogation en matière de responsabilité, les prestataires de services d'hébergement sont tenus d'agir promptement pour retirer les informations illicites qu'ils stockent ou rendre l'accès à celles-ci impossible dès qu'ils en ont effectivement connaissance et, en ce qui concerne une demande en dommages et intérêts, dès qu'ils ont connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente. Ils peuvent notamment en avoir connaissance grâce aux notifications qui leur sont transmises. En tant que telle, la directive 2000/31/CE constitue la base pour l'élaboration de procédures visant à retirer les informations illicites et à rendre l'accès à celles-ci impossible. Cette directive prévoit également la possibilité pour les États membres d'exiger des prestataires de services concernés qu'ils appliquent un devoir de vigilance à l'égard des contenus illicites qu'ils pourraient stocker.
- (9) Lorsqu'ils prennent des mesures relatives aux contenus illicites en ligne, les États membres doivent respecter le principe du pays d'origine établi dans la directive 2000/31/CE. En conséquence, ils ne peuvent, pour des raisons relevant du domaine coordonné spécifié dans ladite directive, restreindre la libre prestation des services de la société de l'information par des prestataires établis dans un autre État membre, sous réserve toutefois de la possibilité de dérogations sous certaines conditions énoncées dans cette directive.
- (10) En outre, un certain nombre d'autres actes de l'Union prévoient un cadre juridique pour certains types spécifiques de contenus illicites qui sont disponibles et diffusés en ligne. En particulier, la directive 2011/93/UE du Parlement européen et du Conseil<sup>5</sup> exige des États membres qu'ils prennent des mesures pour supprimer les pages internet contenant ou diffusant de la pédopornographie et leur permet de bloquer l'accès aux pages internet concernées, sous réserve de certaines garanties. La directive (UE) 2017/541 du Parlement européen et du Conseil<sup>6</sup>, qui doit être transposée en droit national au plus tard le 8 septembre 2018, comporte des dispositions similaires en ce qui concerne les contenus en ligne constituant une provocation publique à commettre une infraction terroriste. En outre, la directive (UE) 2017/541 établit aussi des règles minimales relatives à la définition des infractions pénales dans le domaine des infractions terroristes, des infractions liées à un groupe terroriste et des infractions liées à des activités terroristes. En vertu de la directive 2004/48/CE du Parlement européen et du Conseil relative au respect des droits de propriété intellectuelle<sup>7</sup>, les autorités judiciaires compétentes peuvent émettre des injonctions à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit de propriété intellectuelle.

---

<sup>4</sup> Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (JO L 178 du 17.7.2000, p. 1).

<sup>5</sup> Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO L 335 du 17.12.2011, p. 1).

<sup>6</sup> Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

<sup>7</sup> Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle (JO L 157 du 30.4.2004, p. 45).

- (11) En particulier, dans ce contexte, outre les mesures volontaires prises par certains prestataires de services en ligne, quelques États membres ont adopté des règles sur les procédures de «notification et action» depuis l'adoption de la directive 2000/31/CE. D'autres États membres envisagent d'adopter de telles règles. De manière générale, ces procédures visent à faciliter la notification de contenus que la partie notifiante considère comme illicites au prestataire de services d'hébergement concerné («notification»), en fonction de quoi ce prestataire peut décider s'il accepte ou non ce point de vue et souhaite retirer ces contenus ou rendre l'accès à ceux-ci impossible («action»). On constate des différences croissantes entre les règles nationales à cet égard. Il en ressort que les prestataires de services concernés peuvent être soumis à un ensemble d'exigences juridiques qui diffèrent quant à leur contenu et leur portée.
- (12) Dans l'intérêt du marché intérieur et de l'efficacité de la lutte contre les contenus illicites en ligne, et afin de préserver l'approche équilibrée que la directive 2000/31/CE vise à assurer, il est nécessaire de définir certains principes fondamentaux qui devraient guider l'action des États membres et des prestataires de services concernés à cet égard.
- (13) Ces principes devraient être définis et appliqués dans le plein respect des droits fondamentaux protégés par l'ordre juridique de l'Union et, en particulier, ceux consacrés par la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»). Il faudrait mener la lutte contre les contenus illicites en ligne en prenant des mesures de sauvegarde solides et appropriées pour assurer la protection des divers droits fondamentaux en jeu de l'ensemble des parties concernées. Au rang de ces droits figurent, selon le cas, la liberté d'expression, y compris la liberté de recevoir et de communiquer des informations, les droits au respect de la vie privée et à la protection des données à caractère personnel ainsi que le droit à une protection juridictionnelle effective des utilisateurs des services concernés. Ces droits peuvent aussi englober la liberté d'entreprise, et notamment la liberté contractuelle, des prestataires de services d'hébergement, ainsi que les droits de l'enfant et les droits à la protection de la propriété, y compris la propriété intellectuelle, à la dignité humaine et à la non-discrimination de certaines autres parties concernées. En particulier, les décisions prises par les prestataires de services d'hébergement de retirer des contenus qu'ils stockent ou d'en rendre l'accès impossible devraient tenir dûment compte des droits fondamentaux et des intérêts légitimes de leurs utilisateurs ainsi que du rôle central que ces prestataires ont tendance à jouer pour faciliter le débat public et la diffusion et la réception d'informations factuelles, d'opinions et d'idées dans le respect de la loi.
- (14) Conformément à l'approche horizontale sous-tendant l'exemption de responsabilité prévue à l'article 14 de la directive 2000/31/CE, la présente recommandation devrait être appliquée à tous les types de contenus qui ne sont pas conformes à la législation de l'Union ou aux législations des États membres, quels que soient l'objet précis ou la nature de ces législations. À cet égard, il suffit de tenir compte des législations des États membres concernés par la fourniture de services en cause, à savoir celles des États membres dont le territoire est celui où le prestataire de services d'hébergement est établi ou celui où les services sont fournis. En outre, lors de la mise en œuvre de la présente recommandation, il conviendrait de tenir dûment compte de la gravité des contenus illicites, ainsi que de tout type de préjudice potentiel causé par ces derniers – deux éléments qui influencent fortement la rapidité des éventuelles mesures prises –, ainsi que de ce qui peut raisonnablement être attendu des prestataires de services d'hébergement, compte tenu, au besoin, de l'état d'avancement des technologies et de

la possibilité d'y recourir. Les différences pouvant exister entre les divers types de contenus illicites et les mesures à prendre pour lutter contre ces derniers devraient également être dûment prises en compte.

- (15) Les prestataires de services d'hébergement jouent un rôle particulièrement important dans la lutte contre les contenus illicites en ligne, puisqu'ils stockent des informations fournies par leurs utilisateurs et à la demande de ces derniers, et permettent à d'autres utilisateurs d'y accéder, souvent à grande échelle. La présente recommandation concerne donc principalement les activités et les responsabilités de ces prestataires. Toutefois, lorsque cela se justifie, les recommandations formulées peuvent également s'appliquer mutatis mutandis en lien avec d'autres prestataires de services en ligne concernés. La présente recommandation ayant pour objectif de faire face aux risques liés à des contenus illicites en ligne qui nuisent aux consommateurs dans l'Union, elle porte sur les activités de l'ensemble des prestataires de services d'hébergement, qu'ils soient établis dans l'Union ou dans un pays tiers, pour autant que leurs activités soient orientées vers des consommateurs résidant dans l'Union.
- (16) Parmi les principaux moyens de lutte contre les contenus illicites en ligne figurent les mécanismes de notification de contenus considérés comme illicites aux prestataires de services d'hébergement. Ce type de mécanisme devrait faciliter la notification par l'ensemble des particuliers ou des entités qui souhaitent entreprendre une démarche en ce sens. Dès lors, les mécanismes en question devraient être faciles d'accès et d'utilisation pour tous les utilisateurs. Cependant, les prestataires de services d'hébergement devraient conserver une flexibilité, par exemple en ce qui concerne la forme des notifications ou la technologie à utiliser, de manière à permettre l'application de solutions efficaces et à éviter que des charges disproportionnées ne pèsent sur lesdits prestataires.
- (17) Conformément à la jurisprudence de la Cour de justice relative à l'article 14 de la directive 2000/31/CE, les notifications devraient être suffisamment précises et correctement étayées pour permettre au prestataire de services d'hébergement qui les reçoit de prendre une décision éclairée et rapide quant à la suite à donner à la notification. Par conséquent, il conviendrait de veiller, dans la mesure du possible, au respect de cette norme. Cependant, le fait qu'une notification donnée permette ou non à un prestataire d'avoir les connaissances visées à l'article 14 de ladite directive doit être apprécié en fonction des particularités de chaque cas examiné, en gardant à l'esprit que de telles connaissances peuvent également s'obtenir par d'autres moyens que les notifications.
- (18) Il n'est généralement pas nécessaire que le prestataire de services d'hébergement dispose des coordonnées du notifiant pour prendre une décision éclairée et rapide quant à la suite à donner à la notification reçue. Si, pour l'envoi d'une notification, il était exigé au préalable de communiquer des coordonnées, cette condition constituerait un obstacle à la notification. Il est toutefois nécessaire d'indiquer des coordonnées pour que le prestataire de services d'hébergement soit en mesure de fournir un retour d'information. La transmission des coordonnées du notifiant devrait donc être une possibilité pour celui-ci, et non une obligation.
- (19) Afin d'accroître la transparence et l'exactitude des mécanismes de notification et d'action, et de permettre les recours si nécessaire, les prestataires de services d'hébergement devraient, lorsqu'ils sont en possession des coordonnées des notifiants et/ou des fournisseurs de contenus, informer à temps et correctement les personnes concernées des mesures prises dans le cadre de ces mécanismes, notamment de leurs

décisions au sujet des demandes visant à retirer des contenus ou à en rendre l'accès impossible. Les informations à fournir devraient être proportionnées, c'est-à-dire correspondre aux remarques formulées par les personnes concernées dans leurs notifications ou contre-notifications; dans le même temps, des solutions adaptées et différenciées devraient pouvoir être adoptées et la charge ne devrait pas être excessive pour les prestataires.

- (20) Afin d'assurer la transparence et l'équité et d'éviter le retrait non souhaité de contenus qui ne sont pas illicites, les fournisseurs de contenus devraient, par principe, être informés de la décision de retirer un contenu stocké à leur demande ou d'en rendre l'accès impossible et avoir la possibilité de contester la décision au moyen d'une contre-notification, afin que la décision en question soit révoquée s'il y a lieu, indépendamment du fait qu'elle ait été prise à la suite d'une notification ou d'un signalement ou dans le cadre de mesures proactives appliquées par le prestataire de services d'hébergement.
- (21) Cependant, au vu de la nature des contenus en cause, de l'objectif d'une telle procédure de contre-notification et de la charge supplémentaire qu'elle implique pour les prestataires de service d'hébergement, il n'est pas justifié de recommander de fournir ces informations concernant la décision prise et la possibilité de la contester lorsqu'il est évident que le contenu en question est illicite et concerne de graves infractions pénales comportant une menace pour la vie ou la sécurité des personnes, telles que les infractions visées dans les directives (UE) 2017/541 et 2011/93/UE. En outre, dans certains cas, des motifs d'ordre public et de sécurité publique, notamment liés à la prévention et à la détection des infractions pénales, ainsi qu'aux enquêtes et aux poursuites en la matière, peuvent justifier de ne pas transmettre ces informations directement au fournisseur de contenus concerné. Les prestataires de services d'hébergement ne devraient donc pas procéder à la transmission lorsqu'une autorité compétente a introduit une demande à cet effet, fondée sur des motifs d'ordre public et de sécurité publique, aussi longtemps que souhaité par ladite autorité sur la base de ces motifs. Dans la mesure où cela implique une restriction du droit d'être informé dans le cadre du traitement de données à caractère personnel, les conditions applicables énoncées dans le règlement (UE) 2016/679 devraient être respectées.
- (22) Les mécanismes de notification et d'action ne devraient aucunement modifier le droit des parties concernées d'intenter une action en justice conformément à la législation applicable, vis-à-vis de tout contenu considéré comme illicite ou de toute mesure prise à cet égard par des prestataires de services d'hébergement. Des mécanismes de règlement extrajudiciaire des litiges survenant en la matière peuvent constituer un complément important à la procédure judiciaire, notamment lorsqu'ils permettent le règlement efficace, peu coûteux et rapide de ces litiges. Les règlements extrajudiciaires devraient donc être encouragés, à condition que les mécanismes concernés respectent certaines normes, notamment en termes d'équité procédurale, que l'accès des parties à la justice demeure inchangé et que les abus soient évités.
- (23) Pour mieux évaluer l'efficacité des mécanismes de notification et d'action ainsi que celle des autres mesures prises par les prestataires de services d'hébergement à l'égard des contenus considérés comme illicites et pour garantir la prise de responsabilités, une transparence à l'égard du grand public est nécessaire. Les prestataires de services d'hébergement devraient donc publier régulièrement des rapports sur ces mécanismes et autres mesures, qui devraient être suffisamment exhaustifs et détaillés pour donner une vision correcte. Ils devraient également expliquer clairement ex ante, dans leurs



conditions d'utilisation, leurs politiques de retrait des contenus qu'ils stockent, y compris les contenus illicites, ainsi que de blocage de l'accès à ces contenus.

- (24) Outre les mécanismes de notification et d'action, des mesures proactives spécifiques et proportionnées prises volontairement par les prestataires de services d'hébergement, pouvant passer par le recours à des procédés automatisés dans certains cas, peuvent également constituer un élément important dans la lutte contre les contenus illicites en ligne, sans préjudice de l'article 15, paragraphe 1, de la directive 2000/31/CE. En lien avec de telles mesures proactives, il convient de tenir compte de la situation des prestataires de services d'hébergement qui, du fait de leur taille ou de l'échelle à laquelle ils exercent leurs activités, ne disposent que de ressources et d'une expertise limitées, ainsi que de la nécessité d'assortir ces mesures de mesures de sauvegarde efficaces et adéquates.
- (25) Il peut notamment être adéquat de prendre de telles mesures proactives lorsque le caractère illicite du contenu a déjà été établi ou lorsque le type de contenu est tel qu'il n'est pas nécessaire de le contextualiser. L'action peut dépendre également de la nature, de l'ampleur et de la finalité des mesures envisagées, du type de contenu en cause, de la notification ou non de ce contenu par les autorités répressives ou Europol, et des mesures qui ont déjà été prises à l'égard du contenu concerné au motif qu'il est considéré comme illicite. En ce qui concerne plus spécifiquement le matériel à caractère pédopornographique, les prestataires de services d'hébergement devraient prendre des mesures proactives visant à détecter ce type de matériel et à en prévenir la diffusion, conformément aux engagements pris dans le cadre de l'Alliance mondiale contre la pédopornographie sur l'internet.
- (26) Dans ce contexte, la Commission a présenté dans sa communication du 28 septembre 2017 sur la lutte contre le contenu illicite en ligne le point de vue selon lequel l'adoption de ce type de mesures proactives volontaires ne conduit pas automatiquement le prestataire de services d'hébergement concerné à perdre le bénéfice de l'exemption de responsabilité prévue à l'article 14 de la directive 2000/31/CE.
- (27) Il est essentiel que toutes les mesures adoptées pour lutter contre des contenus illicites en ligne soient soumises à des mesures de sauvegarde efficaces et adéquates destinées à faire en sorte que les prestataires de services d'hébergement agissent avec diligence et de manière proportionnée lorsqu'ils définissent et appliquent leurs politiques à l'égard de tout contenu qu'ils stockent, y compris les contenus illicites, afin de veiller notamment à ce que les utilisateurs puissent recevoir et transmettre librement des informations en ligne dans le respect de la législation applicable. Outre les garanties établies dans la législation applicable, concernant par exemple la protection des données à caractère personnel, des mesures de sauvegarde particulières, comme la surveillance et les vérifications humaines, devraient être prévues et appliquées lorsque cela se justifie dans le cadre de l'utilisation de procédés automatisés, afin d'éviter des décisions non souhaitées et erronées.
- (28) Il convient d'assurer une coopération fluide, efficace et appropriée entre les autorités compétentes et les prestataires de services d'hébergement dans la lutte contre les contenus illicites en ligne. Cette coopération pourrait bénéficier du soutien d'Europol lorsque cela se justifie, par exemple dans la lutte contre le terrorisme et contre les abus sexuels et l'exploitation sexuelle des enfants, la pédopornographie et la sollicitation d'enfants à des fins sexuelles. Pour faciliter cette coopération, les États membres et les prestataires de services d'hébergement devraient désigner des points de contact, et des

procédures devraient être mises en place pour que les notifications transmises par ces autorités soient traitées en priorité et avec un degré de confiance adéquat quant à leur exactitude, compte tenu de l'expertise spécifique et des responsabilités de ces autorités. Afin de lutter efficacement contre certaines infractions pénales particulièrement graves, telles que les infractions visées dans les directives (UE) 2017/541 et 2011/93/UE, qui pourraient être portées à la connaissance des prestataires de services d'hébergement dans l'exercice de leurs activités, les États membres devraient être encouragés à faire usage de la possibilité prévue à l'article 15, paragraphe 2, de la directive 2000/31/CE d'instaurer en droit des obligations d'information, dans le respect de la législation applicable, notamment le règlement (UE) 2016/679 du Parlement européen et du Conseil<sup>8</sup>.

- (29) Outre les autorités compétentes, certains particuliers ou certaines entités, y compris des organisations non gouvernementales et des associations professionnelles, pourraient également posséder une expertise particulière et vouloir prendre, sur une base volontaire, certaines responsabilités liées à la lutte contre les contenus illicites en ligne. Compte tenu de leur valeur ajoutée et du nombre parfois élevé de notifications concernées, il convient d'encourager la coopération entre de tels signaleurs de confiance et les prestataires de services d'hébergement, notamment en traitant également les notifications qu'ils communiquent en priorité et avec un degré de confiance adéquat quant à leur exactitude. Toutefois, conformément à leur statut particulier, cette coopération ne devrait être ouverte qu'aux personnes et entités qui respectent les valeurs sur lesquelles l'Union est fondée, énoncées à l'article 2 du traité sur l'Union européenne, et remplir certaines conditions appropriées, qui devraient en outre être claires et objectives et être mises à la disposition du public.
- (30) La lutte contre les contenus illicites nécessite une approche globale, car ces contenus migrent souvent facilement d'un prestataire de services d'hébergement à un autre et ont tendance à exploiter les maillons les plus faibles de la chaîne. La coopération consistant notamment à partager sur une base volontaire des expériences, des solutions technologiques et des bonnes pratiques est donc essentielle. Cette coopération est particulièrement importante en ce qui concerne les prestataires de services d'hébergement qui, du fait de leur taille ou de l'échelle à laquelle ils exercent leurs activités, ne disposent que de ressources et d'une expertise limitées.
- (31) Le terrorisme consiste à utiliser illégalement et aveuglément des actes de violence et d'intimidation à l'encontre de citoyens. Les terroristes sont devenus de plus en plus tributaires de l'internet pour diffuser leur propagande et ils utilisent souvent des méthodes sophistiquées pour assurer une diffusion large et rapide. Bien que des progrès aient été réalisés, notamment dans le cadre du forum de l'UE sur l'internet, une nécessité urgente persiste de réagir plus rapidement et plus efficacement aux contenus à caractère terroriste en ligne, s'ajoutant à la nécessité que les prestataires de services d'hébergement prenant part au forum de l'UE sur l'internet respectent pleinement leurs engagements en matière d'information effective et exhaustive.
- (32) Eu égard aux particularités liées à la lutte contre les contenus à caractère terroriste en ligne, il convient de compléter les recommandations relatives à la lutte contre les contenus illicites en général par un certain nombre de recommandations concernant

---

<sup>8</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

spécifiquement la lutte contre les contenus à caractère terroriste en ligne, en s'appuyant sur les efforts fournis dans le cadre du forum de l'UE sur l'internet et en les consolidant.

- (33) Compte tenu des risques particulièrement graves liés aux contenus à caractère terroriste et du rôle capital joué par les prestataires de services d'hébergement dans la diffusion de tels contenus, ces prestataires devraient prendre toutes les mesures raisonnables qui s'imposent afin de ne pas permettre la diffusion de contenus à caractère terroriste et, si possible, de ne pas les héberger, sous réserve de la possibilité qui leur est donnée de fixer et d'appliquer leurs conditions d'utilisation et de la nécessité de mesures de sauvegarde efficaces et adéquates, et sans préjudice de l'article 14 de la directive 2000/31/CE.
- (34) Ces mesures devraient notamment consister à coopérer avec les autorités compétentes et Europol pour ce qui est des signalements, qui constituent un mode spécifique de notification aux prestataires de services d'hébergement, adapté aux spécificités de la lutte contre les contenus à caractère terroriste. Lors de l'introduction de signalements, les autorités compétentes et Europol devraient être en mesure de demander le retrait des contenus qu'ils jugent à caractère terroriste ou le blocage de l'accès à ceux-ci, soit sur la base de la législation applicable, soit sur celle des conditions d'utilisation du prestataire de services d'hébergement concerné. Ces mécanismes de signalement devraient s'ajouter aux mécanismes de notification, y compris par des signaleurs de confiance, qui peuvent aussi être utilisés pour signaler des contenus jugés à caractère terroriste.
- (35) Étant donné que les contenus à caractère terroriste sont généralement les plus nuisibles au cours de la première heure qui suit leur apparition en ligne et compte tenu de l'expertise et des responsabilités spécifiques des autorités compétentes et d'Europol, il conviendrait, de manière générale, d'examiner les signalements et d'y donner les suites nécessaires dans l'heure.
- (36) Parmi les mesures destinées à lutter contre les contenus à caractère terroriste devraient également figurer des mesures proactives proportionnées et spécifiques, faisant notamment appel à des procédés automatisés propres à détecter, circonscrire et retirer rapidement tout contenu à caractère terroriste ou à en rendre rapidement l'accès impossible et à faire en sorte que les contenus à caractère terroriste ne réapparaissent pas, sans préjudice de l'article 15, paragraphe 1, de la directive 2000/31/CE. À cet égard, il convient de prendre en compte la nécessité d'assortir ces mesures de mesures de sauvegarde adéquates et efficaces, en particulier celles recommandées au chapitre II de la présente recommandation.
- (37) La coopération, tant entre les différents prestataires de services d'hébergement qu'entre ces derniers et les autorités compétentes, est de la plus haute importance dès lors qu'il s'agit de lutter contre les contenus à caractère terroriste en ligne. En particulier, les outils technologiques qui permettent une détection automatisée des contenus, tels que la base de données d'empreintes numériques, peuvent contribuer à atteindre l'objectif consistant à prévenir la diffusion de contenus à caractère terroriste à travers différents services d'hébergement. Il conviendrait d'encourager une telle coopération, de même que l'élaboration, l'emploi et le partage de tels outils technologiques, en tirant parti de l'expertise d'Europol lorsque cela se justifie. Ces efforts de coopération sont particulièrement importants pour permettre à des prestataires de services d'hébergement qui, du fait de leur taille ou de l'échelle à laquelle ils exercent leurs activités, disposent de ressources et d'une expertise limitées,

de donner suite efficacement et de manière urgente à des signalements et de prendre des mesures proactives, ainsi que recommandé.

- (38) Il convient que le plus grand nombre possible de prestataires de services d'hébergement concernés se joignent à ces efforts de coopération et que l'ensemble des prestataires de services d'hébergement participants contribuent à optimiser et à maximiser l'emploi de ces outils. La conclusion d'accords sur les modalités de travail entre l'ensemble des parties concernées, y compris Europol lorsque cela se justifie, devrait aussi être encouragée, de tels accords pouvant contribuer à mettre en place une approche cohérente et efficace et favoriser l'échange d'expériences et d'expertise en la matière.
- (39) Afin de garantir le respect du droit fondamental relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que la libre circulation de ces données, le traitement desdites données dans le contexte des éventuelles mesures prises pour donner effet à la présente recommandation devrait respecter pleinement les règles sur la protection des données, en particulier le règlement (UE) 2016/679 et la directive (UE) 2016/680 du Parlement européen et du Conseil<sup>9</sup>, et faire l'objet d'un suivi par les autorités de contrôle compétentes.
- (40) La présente recommandation respecte les droits fondamentaux et observe les principes reconnus, en particulier, par la charte. La présente recommandation vise notamment à assurer le respect entier des articles 1<sup>er</sup>, 7, 8, 10, 11, 16, 17, 21, 24 et 47 de la charte.
- (41) La Commission entend suivre de près toutes les mesures prises en réponse à la présente recommandation. Les États membres et les prestataires de services d'hébergement devraient dès lors être disposés à fournir à la Commission, à sa demande, toutes les informations pertinentes pouvant raisonnablement être attendues d'eux en vue de permettre un tel suivi. Sur la base des informations ainsi obtenues et de toutes les autres informations disponibles, y compris des rapports établis sur la base des divers accords volontaires, la Commission évaluera les effets donnés à la présente recommandation et déterminera s'il est ou non nécessaire de prendre des mesures supplémentaires, et notamment de proposer des actes contraignants du droit de l'Union. Compte tenu des particularités et du caractère urgent de la lutte contre les contenus à caractère terroriste en ligne, il importe de réaliser ce suivi et cette évaluation en se fondant sur des informations détaillées et particulièrement rapidement, dans les trois mois suivant la date de publication de la présente recommandation, contre six mois pour les autres contenus illicites,

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

## Chapitre I

### Objet et terminologie

1. Les États membres et les prestataires de services d'hébergement, pour ce qui est des contenus fournis par les fournisseurs de contenus qu'ils stockent à la demande desdits fournisseurs, sont encouragés à prendre des mesures efficaces, appropriées et

---

<sup>9</sup> Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

proportionnées pour lutter contre les contenus illicites en ligne, conformément aux principes exposés dans la présente recommandation et dans le plein respect de la charte, en particulier du droit à la liberté d'expression et d'information, et des autres dispositions applicables du droit de l'Union, notamment en ce qui concerne la protection des données à caractère personnel, la concurrence et le commerce électronique.

2. La présente recommandation s'appuie, en les consolidant, sur les progrès réalisés dans le cadre des accords volontaires conclus entre les prestataires de services d'hébergement et d'autres prestataires de services concernés au regard de divers types de contenus illicites. En matière de terrorisme, elle s'appuie, en les consolidant, sur les progrès réalisés dans le cadre du forum de l'UE sur l'internet.
3. La présente recommandation est sans préjudice des droits et obligations qu'ont les États membres pour ce qui est de prendre des mesures à l'égard des contenus illicites en ligne conformément au droit de l'Union, dont la possibilité donnée aux juridictions ou aux autorités administratives des États membres, conformément à leur système juridique, de demander à des prestataires de services d'hébergement de retirer des contenus illicites ou d'en rendre l'accès impossible. La présente recommandation est également sans préjudice de la position des prestataires de services d'hébergement en vertu de la directive 2000/31/CE et de la possibilité qui leur est donnée de fixer et d'appliquer leurs conditions d'utilisation conformément au droit de l'Union et aux législations des États membres.
4. Aux fins de la présente recommandation, on entend par:
  - (a) «prestataire de services d'hébergement»: un prestataire de services de la société de l'information consistant à stocker des informations fournies par un destinataire du service, à sa demande, au sens de l'article 14 de la directive 2000/31/CE, quel que soit son lieu d'établissement, qui dirige ses activités vers des consommateurs résidant dans l'Union;
  - (b) «contenu illicite»: toute information contraire au droit de l'Union ou au droit de l'État membre concerné;
  - (c) «utilisateur»: toute personne physique ou morale qui est destinataire des services fournis par un prestataire de services d'hébergement;
  - (d) «fournisseur de contenus»: un utilisateur ayant fourni des informations stockées (ou l'ayant été), à sa demande, par un prestataire de services d'hébergement;
  - (e) «notification»: toute communication adressée par un notifiant à un prestataire de services d'hébergement au sujet de contenus stockés par ledit prestataire que le notifiant juge illicites, demandant audit prestataire qu'il retire ces contenus ou en rende l'accès impossible, sur une base volontaire;
  - (f) «notifiant»: une personne ou une entité ayant transmis une notification à un prestataire de services d'hébergement;
  - (g) «signaleur de confiance»: une personne ou une entité considérée par un prestataire de services d'hébergement comme disposant d'une expertise et de responsabilités particulières aux fins de lutter contre les contenus illicites en ligne;
  - (h) «contenu à caractère terroriste»: toute information dont la diffusion constitue une infraction au sens de la directive (UE) 2017/541 ou une infraction terroriste

au sens de la législation de l'État membre concerné, ce qui englobe la diffusion d'informations de ce type émanant de groupes ou d'entités terroristes figurant sur les listes établies par l'Union ou les Nations unies, ou attribuables auxdits groupes ou entités;

- (i) «autorités répressives»: les autorités compétentes chargées par les États membres, conformément à leur législation nationale, de mener à bien des missions répressives à des fins de prévention et de détection des infractions pénales ayant trait à des contenus illicites en ligne, ainsi que d'enquêtes et de poursuites en la matière;
- (j) «autorités compétentes»: les autorités compétentes chargées par les États membres, conformément à leur législation nationale, de mener à bien des missions comprenant notamment la lutte contre les contenus illicites en ligne, et dont font notamment partie les autorités répressives et les autorités administratives chargées de faire respecter la législation applicable dans certains domaines particuliers, indépendamment de la nature ou de l'objet spécifique de cette législation;
- (k) «signalement»: toute communication adressée par une autorité compétente ou Europol à un prestataire de services d'hébergement au sujet de contenus stockés par ledit prestataire que l'autorité compétente ou Europol juge à caractère terroriste, demandant audit prestataire de retirer ces contenus ou d'en rendre l'accès impossible, sur une base volontaire.

## Chapitre II

### Recommandations générales relatives à tous les types de contenus illicites

#### *Introduction et traitement des notifications*

5. Il conviendrait de prévoir des mécanismes de notification. Ces mécanismes devraient être faciles d'accès et d'utilisation et permettre la transmission de notifications par voie électronique.
6. Ces mécanismes devraient permettre et encourager la transmission de notifications suffisamment précises et correctement étayées pour que le prestataire de services d'hébergement concerné soit à même de prendre une décision rapide et en connaissance de cause sur le contenu auquel se rapporte la notification et qu'il puisse notamment se prononcer sur les questions de savoir si ledit contenu doit être jugé illicite ou non et s'il convient de le retirer ou d'en rendre l'accès impossible. Ces mécanismes devraient être conçus de manière à faciliter l'envoi de notifications qui contiennent une explication des raisons pour lesquelles le notifiant considère le contenu comme illicite et une indication claire de l'emplacement du contenu en question.
7. Les notifiants devraient avoir la possibilité, mais non l'obligation, de fournir leurs coordonnées dans une notification. S'ils décident de les fournir, leur anonymat vis-à-vis du fournisseur de contenus devrait être préservé.
8. Dans le cas où le prestataire de services d'hébergement a connaissance des coordonnées du notifiant, ledit prestataire devrait envoyer un accusé de réception au

notifiant et informer ce dernier sans délai injustifié et de manière proportionnée de sa décision à l'égard du contenu dont la notification fait état.

#### *Information des fournisseurs de contenus et contre-notifications*

9. Lorsqu'un prestataire de services d'hébergement décide de retirer un contenu qu'il stocke ou d'en rendre l'accès impossible parce qu'il considère que ce contenu est illicite, indépendamment des moyens employés pour détecter, circonscrire ou retirer ce contenu ou en rendre l'accès impossible, et lorsque ledit prestataire a connaissance des coordonnées du fournisseur de contenus, ce dernier devrait, sans délai injustifié, être informé de manière proportionnée de cette décision et des raisons qui l'ont motivée, ainsi que de la possibilité de contester cette décision, visée au point 11.
10. Toutefois, le point 9 ne devrait pas s'appliquer lorsqu'il est manifeste que le contenu concerné est illicite et se rapporte à des infractions pénales graves comportant une menace pour la vie ou la sécurité de personnes. De plus, les prestataires de services d'hébergement ne devraient pas mettre à disposition les informations visées audit point lorsque et aussi longtemps qu'une autorité compétente formule une demande en ce sens pour des raisons d'ordre public et de sécurité publique, et notamment à des fins de prévention et de détection des infractions pénales, ainsi que d'enquêtes et de poursuites en la matière.
11. Les fournisseurs de contenus devraient avoir la possibilité de contester la décision prise par le prestataire de services d'hébergement, visée au point 9, dans un laps de temps raisonnable, en transmettant à celui-ci une contre-notification. Le mécanisme de contre-notification devrait être facile d'utilisation et permettre la transmission de contre-notifications par voie électronique.
12. Il conviendrait de garantir que les prestataires de services d'hébergement tiennent dûment compte de toute contre-notification qui leur parvient. Lorsqu'une contre-notification contient des raisons amenant le prestataire de services d'hébergement à estimer que le contenu auquel se rapporte ladite contre-notification ne doit pas être considéré comme illicite, ledit prestataire devrait revenir sur sa décision de retirer ce contenu ou d'en rendre l'accès impossible sans délai injustifié, sans préjudice de la possibilité qu'il a de fixer et d'appliquer ses conditions d'utilisation conformément au droit de l'Union et aux législations des États membres.
13. Le fournisseur de contenus qui a introduit une contre-notification, ainsi que le notifiant concerné, devraient, dans le cas où le prestataire de services d'hébergement concerné a connaissance de leurs coordonnées, être informés, sans délai injustifié, de la décision prise par le prestataire de services d'hébergement au sujet du contenu en question.

#### *Règlement extrajudiciaire des litiges*

14. Les États membres sont encouragés à faciliter, lorsque cela se justifie, le règlement extrajudiciaire de litiges portant sur le retrait de contenus illicites ou le blocage de l'accès à ces derniers. Tout mécanisme permettant un tel règlement extrajudiciaire des litiges devrait être facile d'accès, efficace, transparent et impartial, et devrait garantir le caractère équitable des règlements et leur conformité avec le droit applicable. Les tentatives de règlement extrajudiciaire de litiges de ce type ne devraient pas entraver l'accès des parties concernées à la justice.

15. Lorsque des mécanismes de règlement extrajudiciaire des litiges sont disponibles dans l'État membre concerné, les prestataires de services d'hébergement sont encouragés à permettre leur utilisation.

#### *Transparence*

16. Les prestataires de services d'hébergement devraient être encouragés à publier des explications claires, aisément compréhensibles et suffisamment détaillées au sujet de leur politique en matière de retrait de contenus ou de blocage de l'accès à des contenus qu'ils stockent, notamment les contenus considérés comme illicites.
17. Les prestataires de services d'hébergement devraient être encouragés à publier, à intervalles réguliers, et de préférence au moins une fois par an, des rapports sur leurs activités relatives au retrait de contenus considérés comme illicites ou au blocage de l'accès à ces derniers. Ces rapports devraient comporter, en particulier, des informations sur le volume et le type de contenus retirés, sur le nombre de notifications et de contre-notifications reçues, ainsi que sur le délai de réaction.

#### *Mesures proactives*

18. Les prestataires de services d'hébergement devraient être encouragés à prendre, lorsque cela se justifie, des mesures proactives proportionnées et spécifiques en matière de contenus illicites. Ces mesures proactives pourraient comporter le recours à des procédés automatisés de détection de contenus illicites uniquement lorsque c'est approprié et proportionné et sous réserve de mesures de sauvegarde efficaces et adéquates, notamment les mesures de sauvegarde visées aux points 19 et 20.

#### *Mesures de sauvegarde*

19. Afin d'éviter le retrait de contenus qui ne sont pas illicites, sans préjudice de la possibilité que les prestataires de services d'hébergement ont de fixer et d'appliquer leurs conditions d'utilisation conformément au droit de l'Union et aux législations des États membres, des mesures de sauvegarde efficaces et adéquates devraient être prises pour garantir que les prestataires de services d'hébergement agissent avec diligence et de manière proportionnée pour ce qui est des contenus stockés par leurs soins, notamment lorsqu'il s'agit de traiter des notifications et contre-notifications et de décider du retrait éventuel de contenus considérés comme illicites ou du blocage éventuel de l'accès à ces derniers.
20. Lorsque des prestataires de services d'hébergement recourent à des procédés automatisés pour les contenus qu'ils stockent, des mesures de sauvegarde efficaces et adéquates devraient être prévues pour assurer l'exactitude et le bien-fondé des décisions prises au sujet de ces contenus, en particulier les décisions de retrait de contenus considérés comme illicites ou de blocage de l'accès à ces derniers. Ces mesures de sauvegarde devraient notamment consister en une surveillance et en des vérifications humaines, lorsque cela se justifie, et à tout le moins lorsqu'une évaluation détaillée du contexte pertinent est requise pour déterminer si le contenu doit être considéré comme du contenu illicite ou non.

#### *Protection contre les comportements abusifs*

21. Des mesures efficaces et adéquates devraient être prises pour empêcher l'introduction de mauvaise foi - et la prise de mesures y consécutive - de



notifications ou de contre-notifications et toute autre forme de comportement abusif en rapport avec les mesures recommandées en matière de lutte contre les contenus illicites en ligne exposées dans la présente recommandation.

#### *Coopération entre les prestataires de services d'hébergement et les États membres*

22. Les États membres et les prestataires de services d'hébergement devraient désigner des points de contact pour les questions relatives aux contenus illicites en ligne.
23. Des procédures accélérées devraient être mises en place pour traiter les notifications introduites par les autorités compétentes.
24. Les États membres sont encouragés à définir des obligations juridiques imposant aux prestataires de services d'hébergement d'informer promptement les autorités répressives, à des fins de prévention et de détection des infractions pénales et d'enquêtes et de poursuites en la matière, de tout élément de preuve relatif à des infractions pénales graves alléguées comportant une menace pour la vie ou la sécurité de personnes, obtenu dans le cadre de leurs activités en matière de retrait de contenus illicites ou de blocage de l'accès à ces derniers, dans le respect des prescriptions juridiques applicables, en particulier en ce qui concerne la protection des données à caractère personnel, y compris le règlement (UE) 2016/679.

#### *Coopération entre les prestataires de services d'hébergement et les signaleurs de confiance*

25. La coopération entre les prestataires de services d'hébergement et les signaleurs de confiance devrait être encouragée. Plus particulièrement, des procédures accélérées devraient être mises en place pour traiter les notifications introduites par les signaleurs de confiance.
26. Les prestataires de services d'hébergement devraient être encouragés à publier des conditions claires et objectives pour déterminer les personnes ou entités qu'ils considèrent comme des signaleurs de confiance.
27. Ces conditions devraient avoir pour objectif de veiller à ce que les personnes ou entités concernées possèdent l'expertise nécessaire et exercent leurs activités de signaleurs de confiance avec diligence et objectivité, dans le respect des valeurs sur lesquelles l'Union est fondée.

#### *Coopération entre les prestataires de services d'hébergement*

28. Les prestataires de services d'hébergement devraient, lorsque cela se justifie, partager leurs expériences, solutions technologiques et meilleures pratiques en matière de lutte contre les contenus illicites en ligne les uns avec les autres et, en particulier, avec les prestataires de services d'hébergement qui, du fait de leur taille ou de l'échelle à laquelle ils exercent leurs activités, disposent de ressources et d'une expertise limitées, y compris dans le contexte de la coopération existante entre prestataires de services d'hébergement au moyen de codes de conduite, de protocoles d'accord et d'autres accords volontaires.

### Chapitre III

Recommandations spécifiques en matière de contenus à caractère terroriste

### *Généralités*

29. Les recommandations spécifiques en matière de contenus à caractère terroriste exposées dans le présent chapitre s'appliquent en plus des recommandations générales qui figurent au chapitre II.
30. Les prestataires de services d'hébergement devraient expressément indiquer dans leurs conditions d'utilisation qu'ils ne stockeront pas de contenu à caractère terroriste.
31. Les prestataires de services d'hébergement devraient prendre des mesures garantissant qu'ils ne stockent pas de contenu à caractère terroriste, en particulier en ce qui concerne les signalements, les mesures proactives et la coopération conformément aux points 32 à 40.

### *Introduction et traitement des signalements*

32. Les États membres devraient veiller à ce que leurs autorités compétentes soient dotées de la capacité et de ressources suffisantes pour détecter et circonscrire efficacement les contenus à caractère terroriste et pour introduire des signalements auprès des prestataires de services d'hébergement concernés, notamment par l'intermédiaire de leurs unités nationales de signalement de contenus sur l'internet et en coopération avec l'unité de l'UE chargée du signalement des contenus sur l'internet au sein d'Europol.
33. Il conviendrait de prévoir des mécanismes permettant l'introduction de signalements. Des procédures accélérées devraient être mises en place pour traiter les signalements, en particulier les signalements introduits par des unités nationales de signalement de contenus sur l'internet et par l'unité de l'UE chargée du signalement des contenus sur l'internet au sein d'Europol.
34. Les prestataires de services d'hébergement devraient, sans délai injustifié, envoyer des accusés de réception des signalements et informer l'autorité compétente ou Europol des décisions qu'ils ont prises pour le contenu auquel se rapportaient les signalements, en indiquant, selon le cas, le moment où le contenu a été retiré ou le moment où l'accès audit contenu a été rendu impossible, ou la raison pour laquelle ils ont décidé de ne pas retirer le contenu en question ou de ne pas en rendre l'accès impossible.
35. Les prestataires de services d'hébergement devraient évaluer et, lorsque cela se justifie, retirer les contenus identifiés dans les signalements ou en rendre l'accès impossible, en règle générale, dans l'heure qui suit la réception du signalement correspondant.

### *Mesures proactives*

36. Les prestataires de services d'hébergement devraient prendre des mesures proactives proportionnées et spécifiques, notamment en recourant à des procédés automatisés, afin de détecter, de circonscrire et de retirer rapidement tout contenu à caractère terroriste ou d'en rendre rapidement l'accès impossible.
37. Les prestataires de services d'hébergement devraient prendre des mesures proactives proportionnées et spécifiques, notamment en recourant à des procédés automatisés, afin d'empêcher immédiatement les fournisseurs de contenus de republier du contenu

qui a déjà été retiré ou dont l'accès a déjà été rendu impossible du fait qu'il avait été considéré comme du contenu à caractère terroriste.

### *Coopération*

38. Afin d'empêcher la diffusion de contenus à caractère terroriste à travers différents services d'hébergement, les prestataires de services d'hébergement devraient être encouragés à coopérer en partageant des outils technologiques efficaces, appropriés et proportionnés et en les optimisant, y compris les outils qui permettent de détecter automatiquement des contenus de ce type. Lorsque c'est technologiquement possible, tous les formats pertinents par lesquels du contenu à caractère terroriste est diffusé devraient être inclus. Devraient prendre part à une telle coopération, en particulier, les prestataires de services d'hébergement qui, en raison de leur taille ou de l'échelle à laquelle ils exercent leurs activités, disposent de ressources et d'une expertise limitées.
39. Les prestataires de service d'hébergement devraient être encouragés à prendre les mesures nécessaires pour assurer le bon fonctionnement et l'amélioration des outils visés au point 38, notamment en fournissant des éléments d'identification relatifs à tous les contenus considérés comme des contenus à caractère terroriste et en exploitant pleinement les possibilités offertes par ces outils.
40. Les autorités compétentes et les prestataires de services d'hébergement devraient conclure des accords sur les modalités de travail, lorsque cela se justifie également avec Europol, au sujet de questions relatives aux contenus à caractère terroriste en ligne, notamment pour mieux comprendre les activités terroristes en ligne, améliorer les mécanismes de signalement, éviter de multiplier inutilement les efforts et faciliter les demandes des autorités répressives aux fins d'enquêtes pénales en matière de terrorisme.

## Chapitre IV

### Communication d'informations

41. Les États membres devraient, à intervalles réguliers et de préférence tous les trois mois, rendre compte à la Commission des signalements transmis par leurs autorités compétentes et des décisions prises par les prestataires de services d'hébergement à la suite de ces signalements, ainsi que de leur coopération avec les prestataires de services d'hébergement pour ce qui est de la lutte contre les contenus à caractère terroriste.
42. Afin de permettre le suivi des effets donnés à la présente recommandation en ce qui concerne les contenus à caractère terroriste au plus tard trois mois à compter de la date de sa publication, les prestataires de services d'hébergement devraient présenter à la Commission, dès que celle-ci en fait la demande, toutes les informations pertinentes permettant d'effectuer un tel suivi. Ces informations peuvent notamment inclure des renseignements sur le volume de contenus qui ont été retirés ou auxquels l'accès a été rendu impossible, soit à la suite de signalements ou de notifications, soit à la suite de la prise de mesures proactives et de l'utilisation de procédés automatisés. Elles peuvent également comporter des renseignements sur le nombre de signalements reçus et le délai de réaction, ainsi que sur le volume de contenus dont la publication ou la republication a pu être empêchée grâce au recours à des procédés automatisés de détection de contenus et d'autres outils technologiques.

43. Afin de permettre le suivi des effets donnés à la présente recommandation en ce qui concerne les contenus illicites, autres que les contenus à caractère terroriste, au plus tard six mois à compter de la date de sa publication, les États membres et les prestataires de services d'hébergement devraient présenter à la Commission, dès que celle-ci en fait la demande, toutes les informations pertinentes permettant d'effectuer un tel suivi.

Fait à Bruxelles, le 1.3.2018

*Par la Commission*

*Membre de la Commission*