

Bruxelles, le 7 décembre 2018
(OR. en)

15336/18

Dossier interinstitutionnel:
2018/0331(COD)

CT 198
ENFOPOL 605
JAI 1264
COTER 175
CYBER 313
TELECOM 461
FREMP 222
AUDIO 121
DROIPEN 199
CODEC 2270

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	6 décembre 2018
Destinataire:	délégations
N° doc. préc.:	14978/18 + COR 1
N° doc. Cion:	12129/18 + ADD 1-3
Objet:	Proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne - orientation générale

Lors de sa session du 6 décembre 2018, le Conseil est parvenu à un accord sur une orientation générale, dont le texte figure en annexe.

Les modifications apportées à la proposition de la Commission sont indiquées par des *caractères gras/italiques* pour les ajouts et par des crochets [...] pour les suppressions.

[...]

[...] *Projet*

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne

[...]

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen¹,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

- (1) Le présent règlement vise à assurer le bon fonctionnement du marché unique numérique dans une société ouverte et démocratique, en évitant l'utilisation abusive des services d'hébergement à des fins terroristes. Il convient d'améliorer le fonctionnement du marché unique numérique par le renforcement de la sécurité juridique pour les fournisseurs de services d'hébergement, ce qui renforcera la confiance des utilisateurs dans l'environnement en ligne, et par la consolidation des garanties en matière de liberté d'expression et d'information.

¹ JO C du , p. .

- (2) Les fournisseurs de services d'hébergement sur l'internet jouent un rôle essentiel dans l'économie numérique en mettant en relation les entreprises et les citoyens et en facilitant le débat public ainsi que la diffusion et la réception d'informations factuelles, d'opinions et d'idées, et contribuent de manière significative à l'innovation, à la croissance économique et à la création d'emplois dans l'Union. Leurs services font cependant parfois l'objet d'un détournement par des tiers pour exercer des activités illégales en ligne. L'utilisation abusive des services d'hébergement par des groupes terroristes et leurs sympathisants pour diffuser des contenus à caractère terroriste dans le but de propager leur message, de radicaliser et d'attirer de nouvelles recrues, ainsi que de faciliter et diriger des activités terroristes est particulièrement préoccupante.
- (3) La présence de contenus à caractère terroriste en ligne a de graves conséquences négatives pour les utilisateurs, les citoyens et la société en général ainsi que pour les fournisseurs de services en ligne qui hébergent ce type de contenus car cela nuit à la confiance de leurs utilisateurs et érode leurs modèles commerciaux. Étant donné le rôle central qu'ils jouent et les moyens technologiques associés aux services qu'ils fournissent, il incombe aux fournisseurs de services en ligne d'assumer certaines responsabilités sociétales afin de protéger leurs services contre une utilisation abusive par des terroristes et de contribuer à la lutte contre les contenus à caractère terroriste diffusés par l'intermédiaire de leurs services.
- (4) Les efforts de lutte contre les contenus à caractère terroriste ont commencé à être déployés au niveau de l'Union en 2015 dans le cadre d'une coopération volontaire entre les États membres et les fournisseurs de services d'hébergement; il y a lieu de les compléter par un cadre législatif clair afin de réduire davantage l'accessibilité des contenus à caractère terroriste en ligne et de s'attaquer de manière adéquate à un problème en constante évolution. Ce cadre législatif s'appuierait sur les efforts volontaires existants, qui ont été intensifiés par la recommandation (UE) 2018/334 de la Commission², et répond aux appels lancés par le Parlement européen afin de renforcer les mesures visant à lutter contre les contenus illégaux et dangereux et par le Conseil européen afin d'améliorer la détection automatique et la suppression des contenus qui incitent à commettre des actes terroristes.

² Recommandation (UE) 2018/334 de la Commission du 1^{er} mars 2018 sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne (JO L 63 du 6.3.2018, p. 50).

- (5) L'application du présent règlement ne devrait pas avoir d'incidence sur l'application de l'article 14 de la directive 2000/31/CE³. En particulier, aucune des mesures prises par le fournisseur de service d'hébergement en application du présent règlement, y compris des mesures proactives, ne devrait par elle-même entraîner la perte par ce fournisseur de services du bénéfice de l'exemption de responsabilité à cet article. Le présent règlement ne modifie en rien les pouvoirs dont disposent les autorités et les juridictions nationales pour établir la responsabilité des fournisseurs de services d'hébergement dans des cas spécifiques lorsque les conditions prévues à l'article 14 de la directive 2000/31/CE pour bénéficier de l'exemption de responsabilité ne sont pas réunies. ***Le présent règlement ne s'applique pas aux activités liées à la sécurité nationale, car cette dernière reste de la seule responsabilité de chaque État membre.***
- (6) Le présent règlement instaure des règles visant à empêcher l'utilisation abusive de services d'hébergement pour la diffusion de contenus à caractère terroriste en ligne afin de garantir le bon fonctionnement du marché intérieur, 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.

³ 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 ("directive sur le commerce électronique") (JO L 178 du 17.7.2000, p. 1).

- (7) Le présent règlement contribue à la protection de la sécurité publique tout en mettant en place des garanties appropriées et solides qui permettent d'assurer la protection des droits fondamentaux en jeu. Au rang de ces droits figurent les droits au respect de la vie privée et à la protection des données à caractère personnel, le droit à une protection juridictionnelle effective, le droit à la liberté d'expression, y compris la liberté de recevoir et de communiquer des informations, la liberté d'entreprise et le principe de non-discrimination. Les autorités compétentes et les fournisseurs de services d'hébergement devraient uniquement adopter les mesures qui sont nécessaires, appropriées et proportionnées au sein d'une société démocratique, en tenant compte de l'importance particulière accordée à la liberté d'expression et d'information, ***ainsi qu'à la liberté de la presse et au pluralisme des médias***, qui constituent[...] [...] les fondements essentiels d'une société pluraliste et démocratique et figurent parmi les valeurs sur lesquelles l'Union est fondée. Les mesures qui constituent une ingérence dans la liberté d'expression et d'information devraient être strictement ciblées, en ce sens qu'elles doivent servir à empêcher la diffusion de contenus à caractère terroriste sans que cela n'affecte le droit de recevoir et de communiquer légalement des informations, en tenant compte du rôle central que jouent les fournisseurs de services d'hébergement pour faciliter le débat public ainsi que la diffusion et la réception d'informations factuelles, d'opinions et d'idées dans le cadre de la loi.
- (8) Le droit à un recours effectif est consacré à l'article 19 du TUE et à l'article 47 de la Charte des droits fondamentaux de l'Union européenne. Toute personne physique ou morale a droit à un recours juridictionnel effectif devant la juridiction nationale compétente contre toute mesure prise en application du présent règlement susceptible de porter atteinte aux droits de cette personne. Ce droit inclut, en particulier, la possibilité pour les fournisseurs de services d'hébergement et les fournisseurs de contenus de contester de manière effective une injonction de suppression émise par les autorités d'un État membre devant la juridiction de celui-ci ***ainsi que la possibilité pour les fournisseurs de services d'hébergement de contester une décision imposant des mesures proactives ou des sanctions devant la juridiction de l'État membre dans lequel ils sont établis ou disposent d'un représentant légal.***

- (9) Afin de clarifier les actions que tant les fournisseurs de services d'hébergement que les autorités compétentes devraient prendre pour éviter la diffusion de contenus à caractère terroriste en ligne, il convient que le présent règlement établisse une définition des contenus à caractère terroriste à des fins de prévention en s'appuyant sur la définition des infractions terroristes énoncée par la directive (UE) 2017/541 du Parlement européen et du Conseil⁴. Étant donné la nécessité de s'attaquer à la propagande terroriste en ligne la plus nuisible, cette définition devrait inclure le matériel [...] qui incite, encourage ou soutient la commission d'infractions terroristes ou la participation à de telles infractions, [...] ou encourage la participation aux activités d'un groupe terroriste. [...] ***La définition englobe les contenus qui donnent des indications pour la fabrication et l'utilisation d'explosifs, d'armes à feu ou d'autres armes ou substances nocives ou dangereuses ainsi que de substances CBRN, ou en rapport avec d'autres méthodes et techniques, y compris le choix de cibles, aux fins de la commission d'infractions terroristes.*** Ce [...] matériel comprend notamment du texte, des images, des enregistrements sonores et des vidéos. Lorsqu'elles évaluent si un contenu constitue un contenu à caractère terroriste au sens du présent règlement, les autorités compétentes ainsi que les fournisseurs de services d'hébergement devraient tenir compte de facteurs tels que la nature et la formulation des messages, le contexte dans lequel ces messages sont émis et s'ils risquent d'avoir des conséquences néfastes, portant ainsi atteinte à la sécurité et à la sûreté des personnes. Le fait que ce matériel a été produit ou diffusé par une organisation ou une personne inscrite sur la liste des entités terroristes établie par l'UE ou est attribué à une telle organisation ou personne constitue un élément important de l'évaluation. Les contenus diffusés à des fins pédagogiques, [...] ***de contre-discours*** ou de recherche devraient être protégés de manière adéquate ***et veiller à un juste équilibre entre la protection des droits fondamentaux, y compris en particulier la liberté d'expression et d'information, et les exigences de la sécurité publique.*** Lorsque le matériel diffusé est publié sous la responsabilité éditoriale du fournisseur de contenus, toute décision relative à la suppression de tels contenus devrait tenir compte des normes journalistiques arrêtées dans la réglementation de la presse ou des médias conformément au droit de l'Union ainsi qu'au droit à la liberté d'expression et au droit à la liberté et au pluralisme des médias, consacrés à l'article 11 de la Charte des droits fondamentaux. En outre, l'expression d'opinions radicales, polémiques ou controversées dans le cadre du débat public sur des questions politiques sensibles ne devrait pas être considérée comme du contenu à caractère terroriste.

⁴ 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).

- (10) Afin de couvrir les services d'hébergement en ligne par l'intermédiaire desquels des contenus à caractère terroriste sont diffusés, le présent règlement devrait s'appliquer aux services de la société de l'information qui stockent des informations *et du matériel* fournis par un destinataire de ces services à sa demande et en mettant les informations *et le matériel* stockés à la disposition de tiers, indépendamment de la nature purement technique, automatique ou passive de cette activité. [...] ***Le stockage de contenus consiste à détenir des données dans la mémoire d'un serveur physique ou virtuel; cela exclut du champ d'application les services de simple transport et autres services de communication électronique au sens du [code des communications électroniques européen] ou les fournisseurs de services de mise en cache, ou d'autres services fournis au niveau d'autres couches de l'infrastructure internet, tels que les registres ou bureaux d'enregistrement, les systèmes de noms de domaines (DNS) ou services adjacents, tels que les services de protection des services de paiement ou de protection contre les attaques par déni de service distribué. En outre, les informations doivent être stockées à la demande du fournisseur de contenus; seuls les services pour lesquels le fournisseur de contenus est le destinataire direct relèvent du champ d'application. Enfin, les informations stockées sont rendues accessibles à des tiers, c'est-à-dire tout utilisateur tiers qui n'est pas le fournisseur de contenus. Les services de communications interpersonnelles qui permettent l'échange interpersonnel et interactif d'informations entre un nombre fini de personnes, dans lequel les personnes qui amorcent la communication ou y participent en déterminent le(s) destinataire(s), ne relèvent pas du champ d'application. À titre d'exemple, les fournisseurs de services d'hébergement [...] comprennent les plateformes de médias sociaux, les services de diffusion vidéo en continu, les services de partage de fichiers vidéo, audio et images, les services de partage de fichiers et autres services de stockage et stockage en nuage [...]. Le présent règlement s'applique à l'activité de fourniture de services d'hébergement plutôt qu'au fournisseur en tant que tel ou à son activité dominante, qui peut conjuguer des services d'hébergement et d'autres services qui ne relèvent pas du champ d'application du présent règlement.***

(10 bis) Le présent règlement devrait également s'appliquer aux fournisseurs de services d'hébergement établis en dehors de l'Union mais qui offrent des services au sein de l'Union, puisqu'une proportion considérable des fournisseurs de services d'hébergement exposés à des contenus à caractère terroriste par l'intermédiaire de leurs services sont établis dans des pays tiers. Cela devrait garantir que toutes les entreprises opérant au sein du marché unique numérique respectent les mêmes exigences, indépendamment de leur pays d'établissement. Pour déterminer si un fournisseur de services fournit des services dans l'Union, il est nécessaire d'établir si le fournisseur en question permet à des personnes morales ou physiques d'un ou plusieurs États membres d'utiliser ses services. Toutefois, la simple accessibilité du site internet d'un fournisseur ou d'une adresse électronique et d'autres coordonnées de contact dans un ou plusieurs États membres ne devrait pas constituer, prise isolément, une condition suffisante pour l'application du présent règlement.

(11) L'existence d'un lien étroit avec l'Union devrait être prise en considération pour déterminer le champ d'application du présent règlement. Il y a lieu de considérer qu'un tel lien étroit avec l'Union existe lorsque le fournisseur de services dispose d'un établissement dans l'Union ou, dans le cas contraire, sur la base de l'existence d'un nombre significatif d'utilisateurs dans un ou plusieurs États membres ou du ciblage des activités sur un ou plusieurs États membres. Le ciblage des activités sur un ou plusieurs États membres peut être déterminé sur la base de toutes les circonstances pertinentes, et notamment de facteurs comme l'utilisation d'une langue ou d'une monnaie généralement utilisées dans cet État membre, ou la possibilité de commander des biens ou des services. Le ciblage des activités sur un État membre pourrait également se déduire de la disponibilité d'une application dans la boutique d'applications nationale concernée, de la diffusion de publicités à l'échelle locale ou dans la langue utilisée dans cet État membre, ou de la gestion des relations avec la clientèle, par exemple de la fourniture d'un service clientèle dans la langue utilisée généralement dans cet État membre. Il convient également qu'il existe un lien étroit lorsqu'un fournisseur de services dirige ses activités vers un ou plusieurs États membres comme le prévoit l'article 17, paragraphe 1, point c), du règlement (CE) n° 1215/2012 du Parlement européen et du Conseil⁵. En revanche, la fourniture du service en vue du seul respect de l'interdiction de discrimination énoncée dans le règlement (UE) 2018/302 du Parlement et du Conseil⁶ ne peut être considérée, pour ce seul motif, comme orientant ou ciblant des activités vers un territoire donné au sein de l'Union.

⁵ Règlement (UE) 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (JO L 351 du 20.12.2012, p. 1).

⁶ Règlement (UE) 2018/302 du Parlement européen et du Conseil du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur, et modifiant les règlements (CE) n° 2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE (JO L 601 du 2.3.2018, p. 1).

- (12) Les fournisseurs de services d'hébergement devraient respecter certaines obligations de vigilance afin d'empêcher la diffusion de contenus à caractère terroriste par l'intermédiaire de leurs services. Ces obligations de vigilance ne devraient pas constituer une obligation générale de surveillance. Les fournisseurs de services d'hébergement devraient notamment, lorsqu'ils appliquent le présent règlement, agir d'une manière diligente, proportionnée et non discriminatoire à l'égard des contenus qu'ils stockent, en particulier lorsqu'ils appliquent leurs propres conditions commerciales, en vue d'éviter la suppression de contenus qui ne revêtent pas un caractère terroriste. Supprimer des contenus ou en bloquer l'accès doit être entrepris dans le respect de la liberté d'expression et d'information.
- (13) La procédure et les obligations découlant des injonctions juridiques qui enjoignent aux fournisseurs de services d'hébergement de supprimer des contenus à caractère terroriste ou d'en bloquer l'accès, à la suite d'une évaluation par les autorités compétentes, devraient être harmonisées. La désignation des autorités compétentes devrait incomber aux États membres, qui devraient être libres d'assigner cette tâche aux autorités administratives, répressives ou judiciaires de leur choix. Étant donné la vitesse à laquelle les contenus à caractère terroriste sont diffusés dans l'ensemble des services en ligne, la présente disposition impose aux fournisseurs de services d'hébergement l'obligation de veiller à ce que les contenus à caractère terroriste concernés par une injonction de suppression soient supprimés ou que l'accès à ces contenus soit bloqué dans l'heure qui suit la réception de cette injonction. *Sans préjudice de l'obligation de conserver des données au titre de l'article 7 du présent règlement, ou du [projet de législation sur les preuves électroniques], il incombe aux fournisseurs de service d'hébergement de décider s'il convient de supprimer les contenus en question ou d'en bloquer l'accès pour les utilisateurs dans l'Union. Cela devrait avoir pour effet d'empêcher l'accès ou du moins de le rendre difficile et de décourager sérieusement les internautes qui utilisent leurs services d'accéder aux contenus dont l'accès a été bloqué.*

(13 bis) L'injonction de suppression devrait comprendre une classification du contenu concerné en tant que contenu à caractère terroriste et comporter des informations suffisantes de manière à localiser les contenus, par la fourniture d'une adresse URL et de toute autre information supplémentaire, telle qu'une capture d'écran du contenu en question. Sur demande, l'autorité compétente devrait fournir un exposé des motifs complémentaire expliquant pourquoi le contenu est considéré comme étant à caractère terroriste. Il n'est pas nécessaire que les explications fournies contiennent des informations sensibles qui pourraient compromettre les enquêtes. L'exposé des motifs devrait toutefois permettre au fournisseur de services d'hébergement et, à terme, au fournisseur de contenus d'exercer effectivement leur droit au recours juridictionnel.

(14) L'autorité compétente devrait transmettre l'injonction de suppression directement au destinataire et point de contact par tout moyen électronique permettant de laisser une trace écrite dans des conditions qui permettent au fournisseur de services d'en établir l'authenticité, y compris l'exactitude de la date et de l'heure d'envoi et de réception de l'injonction, tel qu'un courrier recommandé, un courrier électronique ou des plateformes sécurisés ou d'autres canaux sécurisés, notamment ceux mis à disposition par le fournisseur de services, conformément aux règles protégeant les données à caractère personnel. Cette exigence peut notamment être satisfaite par l'utilisation de services d'envoi recommandé électronique qualifiés tel que prévu par le règlement (UE) n° 910/2014 du Parlement européen et du Conseil⁷.

⁷ Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

- (15) [...] Le mécanisme de **signalement** [...] consistant à alerter les fournisseurs de services d'hébergement concernant des informations **et du matériel** susceptibles d'être considérés comme des contenus à caractère terroriste, qui permet au fournisseur d'examiner la compatibilité **avec** ses propres conditions commerciales, **constitue un moyen**[...] **particulièrement efficace, rapide et proportionné de sensibiliser les fournisseurs de services d'hébergement à la présence de contenus spécifiques sur leurs services** [...]. Il importe que les fournisseurs de services d'hébergement évaluent ces signalements en priorité et produisent rapidement un retour d'information sur les mesures prises. Les fournisseurs de services d'hébergement restent responsables de la décision finale de supprimer ou non les contenus au motif qu'ils ne sont pas compatibles avec leurs conditions commerciales. Lors de la mise en œuvre du présent règlement en matière de signalement, le mandat d'Europol tel qu'il est défini dans le règlement (UE) 2016/794⁸ reste inchangé.
- (16) Vu l'échelle et la vitesse nécessaires pour identifier et supprimer efficacement des contenus à caractère terroriste, l'adoption de mesures proactives proportionnées, y compris l'utilisation, dans certains cas, de moyens automatisés, constitue un élément essentiel de la lutte contre les contenus à caractère terroriste en ligne. Afin de réduire l'accessibilité de contenus à caractère terroriste sur leurs services, les fournisseurs de services d'hébergement devraient établir s'il est approprié de prendre des mesures proactives en fonction des risques et du niveau d'exposition aux contenus à caractère terroriste ainsi que des effets sur les droits à l'information des tiers et de l'intérêt public. En conséquence, les fournisseurs de services d'hébergement devraient déterminer les mesures appropriées, efficaces et proportionnées qui devraient être mises en place. Cette exigence ne devrait pas impliquer une obligation générale de surveillance. Dans le contexte de cette évaluation, l'absence d'injonctions de suppression et de signalements adressés à un hébergeur est une indication d'un faible **risque** **ou** niveau d'exposition à des contenus à caractère terroriste.

⁸ Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

- (17) Lorsqu'ils mettent en place des mesures proactives, les fournisseurs de services d'hébergement devraient veiller à ce que le droit des utilisateurs à la liberté d'expression et d'information - y compris la liberté de recevoir et de communiquer des informations - soit protégé. Outre les exigences établies dans la législation, y compris la législation relative à la protection des données à caractère personnel, les fournisseurs de services d'hébergement devraient agir avec toute la diligence requise et mettre en œuvre des mesures de sauvegarde, y compris notamment la surveillance et les vérifications humaines, le cas échéant, afin d'éviter des décisions non souhaitées et erronées conduisant à la suppression de contenus qui ne revêtent pas un caractère terroriste. Cela revêt une importance particulière lorsque les fournisseurs de services d'hébergement utilisent des moyens automatisés pour détecter les contenus à caractère terroriste. Toute décision de recourir à des moyens automatisés, qu'elle soit prise par le fournisseur de services d'hébergement lui-même ou à la suite d'une demande émanant de l'autorité compétente, devrait faire l'objet d'une évaluation portant sur la fiabilité de la technologie sous-jacente et des conséquences qui en découlent pour les droits fondamentaux.
- (18) Afin de garantir que les fournisseurs de services d'hébergement exposés à des contenus à caractère terroriste prennent les mesures appropriées pour empêcher l'utilisation abusive de leurs services, les autorités compétentes devraient demander aux fournisseurs de services d'hébergement ayant reçu une injonction de suppression, devenue définitive, de rendre compte des mesures proactives qu'ils auront prises. Il pourrait s'agir de mesures visant à empêcher la remise en ligne de contenus à caractère terroriste qui ont été supprimés ou dont l'accès a été bloqué à la suite d'une injonction de suppression ou d'un signalement qu'ils auraient reçu, par l'utilisation d'outils publics ou privés permettant de les comparer avec des contenus à caractère terroriste connus. Des outils techniques fiables pourraient également permettre d'identifier de nouveaux contenus à caractère terroriste, qu'il s'agisse des outils disponibles sur le marché ou de ceux mis au point par le fournisseur de services d'hébergement. Le fournisseur de services d'hébergement devrait rendre compte des mesures proactives spécifiques mises en place pour permettre à l'autorité compétente de juger si les mesures sont efficaces et proportionnées et de déterminer, lorsque des moyens automatisés sont utilisés, si le fournisseur de service d'hébergement possède les compétences nécessaires en matière de surveillance et de vérification humaines. Pour évaluer l'efficacité et la proportionnalité des mesures, les autorités compétentes devraient tenir compte de paramètres pertinents comme le nombre d'injonctions de suppression et de signalements émis à destination du fournisseur, sa capacité économique et l'incidence de ses services sur la diffusion des contenus à caractère terroriste (par exemple, en tenant compte du nombre d'utilisateurs dans l'Union).

- (19) À la suite de la demande, l'autorité compétente devrait engager un dialogue avec le fournisseur de services d'hébergement sur les mesures proactives qu'il est nécessaire de mettre en place. Le cas échéant, l'autorité compétente devrait imposer l'adoption de mesures proactives appropriées, efficaces et proportionnées lorsqu'elle estime que les mesures prises ne sont pas suffisantes pour se prémunir des risques. Une décision d'imposer de telles mesures proactives ne devrait pas, en principe, conduire à imposer une obligation générale en matière de surveillance, conformément à l'article 15, paragraphe 1, de la directive 2000/31/CE. Au vu des risques particulièrement graves liés à la diffusion de contenus à caractère terroriste, les décisions adoptées par les autorités compétentes sur la base du présent règlement pourraient déroger à l'approche établie à l'article 15, paragraphe 1, de la directive 2000/31/CE en ce qui concerne certaines mesures spécifiques et ciblées dont l'adoption est nécessaire pour des raisons impérieuses de sécurité publique. Avant d'adopter de telles décisions, l'autorité compétente devrait assurer un juste équilibre entre les objectifs d'intérêt général et les droits fondamentaux en jeu, en particulier la liberté d'expression et d'information et la liberté d'entreprise, et fournir des justifications appropriées.
- (20) L'obligation pour les fournisseurs de services d'hébergement de conserver les contenus supprimés et les données connexes devrait être prévue, à des fins spécifiques, et limitée dans le temps à la durée nécessaire. Il y a lieu d'étendre cette exigence de conservation aux données connexes dans la mesure où ces données seraient autrement perdues en raison de la suppression des contenus en question. Les données connexes peuvent comprendre les données relatives aux abonnés, y compris notamment les données relatives à l'identité du fournisseur de contenus, *les données relatives aux transactions et [...]* les données d'accès, y compris par exemple les données concernant la date et l'heure de l'utilisation par le fournisseur de contenus ou la connexion et la déconnexion du service, de même que l'adresse IP allouée par le fournisseur d'accès à l'internet au fournisseur de contenus.

- (21) L'obligation de conserver les contenus à des fins de procédures de réexamen administratif ou de contrôle juridictionnel est nécessaire et justifiée pour garantir l'application de mesures de recours efficaces à l'endroit du fournisseur de contenus dont les contenus ont été supprimés ou dont l'accès a été bloqué, ainsi que pour garantir le rétablissement de ces contenus tels qu'ils se présentaient avant leur suppression, en fonction des résultats de la procédure de réexamen. L'obligation de conserver les contenus à des fins d'enquête et de poursuite est nécessaire et justifiée compte tenu de l'utilité potentielle de ce matériel pour faire échec aux activités terroristes ou les prévenir. Lorsque des entreprises suppriment du matériel ou en bloquent l'accès, en particulier au moyen de leurs propres mesures proactives, et n'en informent pas l'autorité concernée parce qu'elles estiment que cela n'entre pas dans le champ d'application de l'article 13, paragraphe 4, du présent règlement, les autorités répressives pourraient ne pas avoir connaissance de l'existence de ces contenus. Cela justifie également la conservation de contenus à des fins de prévention, de détection, d'enquête et de poursuites en matière d'infractions terroristes. L'exigence de conservation à ces fins se limite aux données susceptibles d'avoir un lien avec des infractions terroristes et peut donc contribuer à la poursuite d'infractions terroristes ou à la prévention de risques graves pour la sécurité publique.
- (22) Par souci de proportionnalité, il y a lieu de limiter la période de conservation à six mois afin de donner aux fournisseurs de contenus le temps suffisant pour engager la procédure de réexamen administratif ou de contrôle juridictionnel et pour permettre aux autorités répressives d'avoir accès aux données pertinentes à des fins d'enquête et de poursuites en matière d'infractions terroristes. À la demande de l'autorité qui procède au réexamen, cette période peut toutefois être prolongée de la durée nécessaire lorsque la procédure de réexamen ou de contrôle juridictionnel est engagée mais non achevée à l'expiration de la période de six mois. Cette durée devrait être suffisante pour permettre aux autorités répressives de conserver les preuves nécessaires en lien avec leurs enquêtes tout en assurant l'équilibre avec les droits fondamentaux concernés.
- (23) Le présent règlement n'a pas d'incidence sur les garanties procédurales ni sur les mesures d'enquêtes relatives à l'accès aux contenus et aux données connexes conservés à des fins d'enquête et de poursuites en matière d'infractions terroristes, qu'elles soient établies dans le cadre de la législation nationale des États membres ou de la législation de l'Union.

- (24) Il est essentiel que les fournisseurs de services d'hébergement appliquent, en ce qui concerne les contenus à caractère terroriste, une politique transparente afin de mieux rendre compte de leurs actions à l'égard de leurs utilisateurs et de renforcer la confiance des citoyens dans le marché unique numérique. Il convient que les fournisseurs de services d'hébergement, **qui sont exposés à des contenus à caractère terroriste**, publient des rapports annuels sur la transparence qui contiennent des informations utiles relatives aux mesures prises en matière de détection, d'identification et de suppression de contenus à caractère terroriste, **dans la mesure où elles ne vont pas à l'encontre des mesures mises en place.**
- (25) Les procédures de réclamation constituent une garantie nécessaire contre la suppression par erreur - **à la suite de mesures prises conformément aux conditions commerciales des fournisseurs de services d'hébergement** - de contenus protégés au titre de la liberté d'expression et d'information. Il y a lieu que les fournisseurs de services d'hébergement mettent en place des dispositifs de réclamation conviviaux et veillent à ce que les réclamations soient traitées rapidement et en toute transparence par rapport au fournisseur de contenus. L'obligation faite au fournisseur de services d'hébergement de rétablir les contenus lorsque ceux-ci ont été supprimés par erreur n'a pas d'incidence sur la possibilité dont disposent les fournisseurs de services d'hébergement d'appliquer, pour d'autres raisons, leurs propres conditions commerciales. **En outre, les fournisseurs de contenus, dont les contenus ont été supprimés à la suite d'une injonction de suppression, devraient avoir le droit à un recours effectif conformément à l'article 19 du TUE et à l'article 47 de la Charte des droits fondamentaux de l'Union européenne.**

- (26) **De manière plus générale**, l[...]article 19 du TUE et l'article 47 de la Charte des droits fondamentaux de l'Union européenne consacrent le droit à une protection juridictionnelle effective, au titre de laquelle les personnes doivent pouvoir connaître les raisons pour lesquelles les contenus qu'elles ont chargés ont été supprimés ou l'accès à ceux-ci rendu impossible. À cette fin, il convient que le fournisseur de services d'hébergement mette à la disposition du fournisseur de contenus des informations utiles, qui permettent à ce dernier de contester la décision. Pour ce faire, une notification au fournisseur de contenus n'est toutefois pas forcément nécessaire. Selon les circonstances, les fournisseurs de services d'hébergement peuvent remplacer les contenus considérés comme revêtant un caractère terroriste par un message indiquant que ceux-ci ont été supprimés ou leur accès bloqué conformément au présent règlement. Il y a lieu, à la demande du fournisseur de contenus, de communiquer à ce dernier de plus amples informations sur les raisons de la suppression, ainsi que sur les possibilités de contestation dont il dispose à cet égard. Lorsque, pour des raisons de sécurité publique, notamment dans le cadre d'une enquête, les autorités compétentes estiment qu'il est inapproprié ou contre-productif de notifier directement la suppression de contenus ou le blocage de l'accès à ces derniers, elles devraient en informer le fournisseur de services d'hébergement.
- (27) Afin d'éviter les doubles emplois et les interférences possibles avec leurs enquêtes, il importe que les autorités compétentes s'informent mutuellement, se coordonnent et coopèrent les unes avec les autres et, le cas échéant, avec Europol [...] **avant** qu'elles émettent des injonctions de suppression ou **lorsqu'elles** adressent des signalements aux fournisseurs de services d'hébergement. Lorsqu'elle décide d'émettre une injonction de suppression, l'autorité compétente devrait tenir dûment compte de toute notification de l'existence d'une interférence avec les intérêts d'une enquête ("déconfliction"). [...] **Lorsqu'elle décide d'émettre une injonction de suppression, l'autorité compétente devrait tenir dûment compte de toute notification de l'existence d'une interférence avec les intérêts d'une enquête ("déconfliction"). Lorsqu'une autorité compétente est informée par une autorité compétente d'un autre État membre de l'existence d'une injonction de suppression, il convient de ne pas émettre une nouvelle injonction faisant double emploi.** Europol pourrait apporter son soutien à la mise en œuvre des dispositions du présent règlement, conformément à son mandat actuel et au cadre juridique existant.

- (28) Afin d'assurer une mise en œuvre efficace et suffisamment cohérente des mesures proactives, il convient que les autorités compétentes des États membres se concertent au sujet des discussions qu'elles ont avec les fournisseurs de services d'hébergement sur l'identification, la mise en œuvre et l'évaluation de mesures proactives spécifiques. De même, une telle coopération est également nécessaire en ce qui concerne l'adoption de règles relatives aux sanctions, ainsi que la mise en œuvre et l'exécution de ces dernières.
- La Commission devrait faciliter une telle coordination et coopération.***
- (29) Il est essentiel que l'autorité compétente au sein de l'État membre responsable de l'instauration des sanctions soit pleinement informée de l'émission des injonctions de suppression et des signalements, ainsi que des échanges ultérieurs entre le fournisseur de services d'hébergement et l'autorité compétente concernée. À cette fin, il convient que les États membres veillent à disposer de canaux et de mécanismes de communication appropriés permettant de partager, en temps voulu, les informations utiles.
- (30) Pour faciliter les échanges rapides entre les autorités compétentes ainsi qu'avec les fournisseurs de services d'hébergement, et pour éviter les doubles emplois, les États membres [...] ***sont incités à*** utiliser les outils ***dédiés*** développés par Europol, tels que l'actuelle application de gestion des signalements sur internet (Irma) ou les outils qui lui succéderont.
- (31) Compte tenu des conséquences particulièrement graves de certains contenus à caractère terroriste, il convient que les fournisseurs de services d'hébergement informent rapidement les autorités de l'État membre concerné ou les autorités compétentes du pays où ils sont établis ou disposent d'un représentant légal de l'existence de toute preuve d'infractions terroristes dont ils ont connaissance. Afin de garantir la proportionnalité, cette obligation est limitée aux infractions terroristes telles que définies à l'article 3, paragraphe 1, de la directive (UE) 2017/541. L'obligation d'informer n'impose pas aux fournisseurs de services d'hébergement l'obligation de rechercher activement de telles preuves. L'État membre concerné est celui qui est compétent pour connaître des enquêtes et des poursuites concernant les infractions terroristes en application de la directive (UE) 2017/541, sur la base de la nationalité de l'auteur ou de la victime potentielle de l'infraction ou du lieu visé par l'acte de terrorisme. En cas de doute, les fournisseurs de services d'hébergement peuvent transmettre les informations à Europol, auquel il revient d'assurer un suivi conformément à son mandat, y compris en transmettant ces informations aux autorités nationales concernées.

- (32) Il y a lieu que les autorités compétentes des États membres soient autorisées à utiliser ces informations pour prendre des mesures d'enquête prévues par la législation de l'État membre ou de l'Union, notamment l'émission d'un ordre de production européen au titre du règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale⁹.
- (33) Tant les fournisseurs de services d'hébergement que les États membres devraient établir des points de contact afin de faciliter le traitement rapide des injonctions de suppression et des signalements. Contrairement au représentant légal, le point de contact sert des objectifs opérationnels. Il convient que le point de contact du fournisseur de services d'hébergement consiste en tout moyen spécifique, *interne ou externalisé*, permettant la soumission électronique des injonctions de suppression et des signalements [...] *ou* en moyens techniques et humains permettant de les traiter rapidement. Le point de contact du fournisseur de services d'hébergement ne doit pas nécessairement être établi dans l'Union et ledit fournisseur est libre de désigner un point de contact existant, à condition que celui-ci soit en mesure de remplir les fonctions prévues par le présent règlement. Afin de garantir que les contenus à caractère terroriste soient supprimés ou que l'accès à ces contenus soit bloqué dans l'heure qui suit la réception d'une injonction de suppression, il importe que *les fournisseurs de services d'hébergement exposés à des contenus à caractère terroriste, attestés par la réception d'une injonction de suppression*, veillent à ce que le point de contact soit joignable 24 heures sur 24 et 7 jours sur 7. Les informations sur le point de contact devraient comprendre des informations concernant la langue dans laquelle le point de contact peut être contacté. Afin de faciliter la communication entre les fournisseurs de services d'hébergement et les autorités compétentes, les fournisseurs de services d'hébergement sont encouragés à permettre la communication dans une des langues officielles de l'Union dans laquelle leurs conditions commerciales sont disponibles.
- (34) Les fournisseurs de services n'étant pas soumis à l'obligation générale de garantir une présence physique sur le territoire de l'Union, il est nécessaire de déterminer clairement l'État membre de la compétence duquel relève le fournisseur de services d'hébergement proposant des services au sein de l'Union. En règle générale, le fournisseur de services d'hébergement relève de la compétence de l'État membre dans lequel il a son établissement principal ou dans lequel il a désigné un représentant légal. *Toutefois, pour des raisons de mise en œuvre effective, d'urgence et de politique publique, tout État membre devrait être compétent pour émettre des injonctions de suppression et adresser des signalements.*

⁹ COM(2018)225 final.

- (35) Les fournisseurs de services d'hébergement qui ne sont pas établis dans l'Union devraient désigner par écrit un représentant légal afin d'assurer le respect et l'exécution des obligations découlant du présent règlement. ***Les fournisseurs de services d'hébergement peuvent recourir à un représentant légal existant, à condition que celui-ci soit en mesure de remplir les fonctions prévues par le présent règlement.***
- (36) Il convient que le représentant légal soit légalement habilité à agir au nom du fournisseur de services d'hébergement.
- (37) Aux fins du présent règlement, les États membres devraient désigner des autorités compétentes. L'obligation de désigner des autorités compétentes n'impose pas nécessairement la création de nouvelles autorités; il peut en effet s'agir d'organismes existants chargés des fonctions prévues par le présent règlement. Celui-ci exige la désignation d'autorités compétentes chargées d'émettre les injonctions de suppression et les signalements et de superviser les mesures proactives, ainsi que d'imposer des sanctions. Il appartient aux États membres de décider du nombre d'autorités qu'ils souhaitent désigner pour remplir ces tâches.

- (38) Des sanctions sont nécessaires pour garantir que les fournisseurs de services d'hébergement mettent effectivement en œuvre les obligations découlant du présent règlement. Il convient que les États membres adoptent des règles en matière de sanctions, **qui peuvent être de nature administrative ou pénale**, y compris, le cas échéant, des lignes directrices pour le calcul des amendes. Des sanctions particulièrement sévères sont prises lorsque le fournisseur de services d'hébergement omet systématiquement de supprimer les contenus à caractère terroriste ou d'en bloquer l'accès dans l'heure qui suit la réception d'une injonction de suppression. Des sanctions seraient possibles dans des cas ponctuels de non-conformité tout en respectant les principes ne bis in idem et de proportionnalité et en veillant à ce que ces sanctions prennent en considération une défaillance systématique. Afin de garantir la sécurité juridique, il y a lieu que le règlement précise dans quelle mesure les obligations pertinentes peuvent faire l'objet de sanctions. Il importe que les sanctions pour non-conformité avec l'article 6 ne soient adoptées qu'en ce qui concerne les obligations découlant d'une demande de communication faite conformément à l'article 6, paragraphe 2, ou d'une décision imposant des mesures proactives supplémentaires en vertu de l'article 6, paragraphe 4. **Lors de l'examen de la nature de l'infraction et au moment de décider de l'application de sanctions, il devrait être tenu pleinement compte des droits fondamentaux, tels que la liberté d'expression.** Au moment de déterminer si des sanctions financières devraient être ou non imposées, il convient de tenir dûment compte des ressources financières du fournisseur. Les États membres veillent à ce que les sanctions n'encouragent pas la suppression de contenus qui ne sont pas à caractère terroriste.
- (39) L'utilisation de modèles normalisés facilite la coopération et l'échange d'informations entre les autorités compétentes et les fournisseurs de services, leur permettant de communiquer plus rapidement et plus efficacement. Il est particulièrement important de garantir une intervention rapide dès la réception d'une injonction de suppression. Les modèles réduisent les coûts de traduction et contribuent à une norme de qualité élevée. De même, les formulaires de réponse devraient permettre un échange normalisé d'informations, ce qui sera particulièrement important lorsque les fournisseurs de services ne sont pas en mesure de se conformer à une demande. Des canaux de transmission authentifiés peuvent garantir l'authenticité de l'injonction de suppression, y compris l'exactitude de la date et de l'heure d'envoi et de réception de l'injonction.

- (40) Afin de pouvoir modifier rapidement, le cas échéant, le contenu des modèles à utiliser aux fins du présent règlement, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en vue de modifier les annexes I, II et III du présent règlement. Afin de pouvoir tenir compte du progrès technologique et du cadre juridique qui y est associé, la Commission devrait également être habilitée à adopter des actes délégués en vue de compléter le présent règlement par des exigences techniques concernant les moyens électroniques que les autorités compétentes doivent utiliser pour transmettre les injonctions de suppression. Il importe notamment que la Commission procède à des consultations appropriées lors de ses travaux préparatoires, notamment au niveau des experts, et que ces consultations respectent les principes énoncés dans l'accord interinstitutionnel "Mieux légiférer" du 13 avril 2016¹⁰. En particulier, pour garantir leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.
- (41) Il y a lieu que les États membres recueillent des informations sur la mise en œuvre de la législation. ***Les États membres peuvent utiliser les rapports sur la transparence des fournisseurs de services d'hébergement et, le cas échéant, les compléter par des informations plus détaillées.*** Il convient d'élaborer un programme détaillé de suivi des réalisations, résultats et effets du présent règlement afin d'étayer une évaluation de la législation.

¹⁰ JO L 123 du 12.5.2016, p. 1.

- (42) Se fondant sur les constatations et conclusions du rapport de mise en œuvre et sur le résultat de l'exercice de suivi, la Commission devrait procéder à une évaluation du présent règlement au plus tôt trois ans après son entrée en vigueur. Cette évaluation devrait reposer sur les cinq critères d'efficacité, d'efficacités, de pertinence, de cohérence et de valeur ajoutée européenne. Elle évaluera le fonctionnement des différentes mesures opérationnelles et techniques prévues par le présent règlement, notamment l'efficacité des mesures visant à améliorer la détection, l'identification et la suppression des contenus à caractère terroriste, l'efficacité des mécanismes de garantie ainsi que les incidences sur les droits et intérêts potentiellement affectés de tiers, y compris un réexamen de l'obligation d'informer les fournisseurs de contenus.
- (43) Étant donné que l'objectif du présent règlement, à savoir garantir le bon fonctionnement du marché unique numérique en prévenant la diffusion de contenus de caractère terroriste, ne peut pas être réalisé de manière suffisante par les États membres et peut donc, en raison de la portée et des effets de la limitation, être mieux réalisé au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

SECTION I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

1. Le présent règlement établit des règles uniformes pour empêcher l'utilisation abusive de services d'hébergement en vue de la diffusion en ligne de contenus à caractère terroriste. Il prévoit notamment:
 - a) des règles relatives aux obligations de vigilance incombant aux fournisseurs de services d'hébergement afin de prévenir la diffusion, par l'intermédiaire de leurs services, de contenus à caractère terroriste et de garantir, le cas échéant, leur suppression rapide;
 - b) un ensemble de mesures à mettre en place par les États membres afin de circonscrire les contenus à caractère terroriste, de permettre leur suppression rapide par les fournisseurs de services d'hébergement et de faciliter la coopération avec les autorités compétentes des autres États membres, les fournisseurs de services d'hébergement et, le cas échéant, les organes compétents de l'Union.
2. Le présent règlement s'applique aux fournisseurs de services d'hébergement qui proposent des services dans l'Union, quel que soit le lieu de leur établissement principal.
3. ***Le présent règlement ne porte pas atteinte à l'obligation de respecter les droits fondamentaux et les principes juridiques fondamentaux consacrés par l'article 6 du traité sur l'Union européenne.***

Article 2

Définitions

Aux fins du présent règlement, on entend par:

- 1) "fournisseur de services d'hébergement", un fournisseur de services de la société de l'information qui consistent à stocker des informations fournies par le fournisseur de contenus à la demande de celui-ci et à mettre ces informations à la disposition de tiers;

- 2) "fournisseur de contenus", un utilisateur qui a fourni des informations stockées (ou l'ayant été), à sa demande, par un fournisseur de services d'hébergement;
- 3) "proposer des services dans l'Union", permettre à des personnes physiques ou morales dans un ou plusieurs États membres d'utiliser les services du fournisseur de services d'hébergement qui a un lien étroit avec cet État membre ou ces États membres, tel que l'établissement du fournisseur de services d'hébergement dans l'Union;

En l'absence d'un tel établissement, l'évaluation d'un lien étroit se fonde sur des critères factuels spécifiques, tels que

- a) ***un*** nombre significatif d'utilisateurs dans un ou plusieurs États membres;
 - b) ***ou le*** ciblage des activités sur un ou plusieurs États membres;
- 4) "infractions terroristes", ***l'un des actes intentionnels énumérés*** [...] à l'article 3, paragraphe 1, de la directive (UE) 2017/541;
 - 5) "contenus à caractère terroriste", [...] ***matériel qui peut contribuer à la commission des actes intentionnels énumérés à l'article 3, paragraphe 1, points a) à i), de la directive (UE) 2017/541, comme suit:***
 - aa) en menaçant de commettre une infraction terroriste;***
 - a) en incitant à la commission d'infractions terroristes, ou en faisant l'apologie de telles infractions, [...] ***par exemple*** [...] ***en glorifiant les actes terroristes***, créant ainsi le risque que de tels actes soient commis;
 - b) ***en sollicitant des personnes ou un groupe de personnes pour commettre*** [...] des infractions terroristes ou y participer [...];

c) en promouvant les activités d'un groupe terroriste, notamment en *sollicitant des personnes ou un groupe de personnes pour* [...] participer ou apporter un soutien *aux activités criminelles d'*[...] un groupe terroriste au sens de l'article 2, paragraphe 3, de la directive (UE) 2017/541;

en fournissant des instructions sur des méthodes ou techniques en vue de la commission d'infractions terroristes;

- 6) "diffusion de contenus à caractère terroriste", le fait de rendre accessibles à des tiers des contenus à caractère terroriste sur les services des fournisseurs de services d'hébergement;
- 7) "conditions commerciales", toutes les modalités, conditions et clauses, quelle que soit leur dénomination ou leur forme, qui régissent la relation contractuelle entre le fournisseur de services d'hébergement et les utilisateurs de ces services;
- 8) "signalement": une notification, par une autorité compétente ou, le cas échéant, un organe compétent de l'Union, à un fournisseur de services d'hébergement, concernant des informations susceptibles d'être considérées comme des contenus à caractère terroriste, destinée à ce que le fournisseur examine, sur une base volontaire, leur compatibilité avec ses propres conditions commerciales afin d'empêcher la diffusion de contenus à caractère terroriste;
- 9) "établissement principal", le siège social ou le siège principal, au sein duquel les principales fonctions financières et le contrôle opérationnel sont exercés *dans l'Union*.

SECTION II

Mesures visant à prévenir la diffusion de contenus à caractère terroriste en ligne

Article 3

Obligations de vigilance

1. Les fournisseurs de services d'hébergement prennent des mesures appropriées, raisonnables et proportionnées, conformément au présent règlement, pour lutter contre la diffusion de contenus à caractère terroriste et protéger les utilisateurs contre ce type de contenus. Ce faisant, ils agissent de manière diligente, proportionnée et non discriminatoire, en tenant dûment compte des droits fondamentaux des utilisateurs et en prenant en considération l'importance fondamentale de la liberté d'expression et d'information dans une société ouverte et démocratique.
2. Les fournisseurs de services d'hébergement inscrivent dans leurs conditions commerciales ***qu'ils ne stockeront pas de contenus terroristes*** ainsi que des dispositions visant à prévenir la diffusion de contenus à caractère terroriste, et appliquent ces dispositions.

Article 4

Injonctions de suppression

1. L'autorité compétente a le pouvoir d[...] émettre une ***injonction de suppression*** enjoignant au fournisseur de services d'hébergement de supprimer les contenus à caractère terroriste ou d'en bloquer l'accès.
2. Les fournisseurs de services d'hébergement suppriment les contenus à caractère terroriste ou en bloquent l'accès dans un délai d'une heure à compter de la réception de l'injonction de suppression.
3. Les injonctions de suppression contiennent les éléments suivants conformément au modèle figurant à l'annexe I:
 - a) l'identification de l'autorité compétente émettant l'injonction de suppression et l'authentification de l'injonction de suppression par l'autorité compétente; [...] ***une évaluation des contenus***, à tout le moins par rapport aux catégories ***pertinentes*** de contenus à caractère terroriste énumérées à l'article 2, paragraphe 5;

- b) une adresse URL (Uniform Resource Locator) et, si nécessaire, des informations supplémentaires permettant d'identifier les contenus en cause;
 - c) une référence au présent règlement en tant que base juridique de l'injonction de suppression;
 - d) l'horodatage de l'émission;
 - e) des informations relatives aux possibilités de recours dont disposent le fournisseur de services d'hébergement et le fournisseur de contenus;
 - f) le cas échéant, la décision, visée à l'article 11, de ne pas divulguer les informations relatives à la suppression de contenus à caractère terroriste ou au blocage de l'accès à ces contenus.
4. L'autorité compétente transmet, sur demande du fournisseur de services d'hébergement ou du fournisseur de contenus, un exposé [...] des motifs ***complémentaire expliquant les raisons pour lesquelles les contenus sont considérés comme des contenus à caractère terroriste***, sans préjudice de l'obligation qui incombe au fournisseur de services d'hébergement de se conformer à l'injonction de suppression dans le délai fixé au paragraphe 2.
5. Les autorités compétentes adressent les injonctions de suppression à l'établissement principal du fournisseur de services d'hébergement ou au représentant légal désigné par ledit fournisseur conformément à l'article 16 et les transmettent au point de contact visé à l'article 14, paragraphe 1. Ces injonctions sont envoyées par des moyens électroniques permettant de laisser une trace écrite dans des conditions qui permettent d'authentifier l'expéditeur, y compris l'exactitude de la date et de l'heure de l'envoi et de la réception de l'injonction.
6. ***Sans retard indu***, l[...]es fournisseurs de services d'hébergement en accusent réception et informent[...] l'autorité compétente de la suppression des contenus à caractère terroriste ou du blocage de l'accès à ces contenus, en indiquant, en particulier, la date et l'heure de l'opération à l'aide du modèle figurant à l'annexe II.

7. Si le fournisseur de services d'hébergement ne peut se conformer à une injonction de suppression pour cause de force majeure ou d'impossibilité de fait qui ne lui est pas imputable, celui-ci en informe, sans retard indu, l'autorité compétente, en exposant les raisons de cette incapacité au moyen du modèle qui figure à l'annexe III. Le délai indiqué au paragraphe 2 s'applique dès que les raisons invoquées n'existent plus.
8. Si le fournisseur de services d'hébergement ne peut se conformer à une injonction de suppression au motif que cette dernière contient des erreurs manifestes ou ne contient pas d'informations suffisantes pour permettre son exécution, il en informe l'autorité compétente, en demandant les précisions nécessaires au moyen du modèle figurant à l'annexe III. Le délai indiqué au paragraphe 2 s'applique dès que les précisions sont fournies.
9. L'autorité compétente qui a émis l'injonction de suppression indique à l'autorité compétente qui supervise la mise en œuvre des mesures proactives visées à l'article 17, paragraphe 1, point c), quand l'injonction de suppression devient définitive. Une injonction de suppression devient définitive lorsqu'elle n'a pas fait l'objet d'un recours dans le délai prévu par le droit national applicable ou lorsqu'elle a été confirmée à la suite d'un recours.

Article 4 bis

Procédure de consultation pour les injonctions de suppression

1. *L'autorité d'émission soumet une copie de l'injonction de suppression à l'autorité compétente visée à l'article 17, paragraphe 1, de l'État membre dans lequel est situé l'établissement principal du fournisseur de services d'hébergement en même temps que la copie est transmise au fournisseur de services d'hébergement conformément à l'article 4, paragraphe 5.*
2. *Dans les cas où l'autorité compétente de l'État membre dans lequel est situé l'établissement principal du fournisseur de services d'hébergement a de bonnes raisons de penser que l'injonction de suppression peut porter atteinte aux intérêts fondamentaux de cet État membre, elle en informe l'autorité compétente qui l'a émise.*
3. *L'autorité d'émission prend ces circonstances en considération et, s'il y a lieu, retire ou adapte l'injonction de suppression.*

Article 5
Signalements

1. L'autorité compétente ou l'organe compétent de l'Union peut adresser un signalement à un fournisseur de services d'hébergement.
2. Les fournisseurs de services d'hébergement mettent en place des mesures opérationnelles et techniques qui facilitent l'évaluation rapide des contenus que les autorités compétentes et, le cas échéant, les organes compétents de l'Union leur transmettent afin qu'ils les examinent sur une base volontaire.
3. Les autorités compétentes adressent le signalement à l'établissement principal du fournisseur de services d'hébergement ou au représentant légal désigné par ledit fournisseur conformément à l'article 16 et le transmettent au point de contact visé à l'article 14, paragraphe 1. Ces signalements sont transmis par voie électronique.
4. Le signalement contient des informations suffisantes [...] **sur** les raisons pour lesquelles les contenus sont considérés comme des contenus à caractère terroriste, **et fournit** une adresse URL et, le cas échéant, des informations supplémentaires permettant d'identifier les contenus à caractère terroriste visés.
5. Le fournisseur de services d'hébergement évalue en priorité les contenus identifiés dans le signalement à l'aune de ses propres conditions commerciales et décide s'il convient de supprimer ces contenus ou d'en bloquer l'accès.
6. Le fournisseur de services d'hébergement informe , **sans retard indu**, [...] l'autorité compétente ou l'organe compétent de l'Union du résultat de l'évaluation et du calendrier des mesures éventuellement prises à la suite du signalement.
7. Lorsque le fournisseur de services d'hébergement estime que le signalement ne contient pas suffisamment d'informations pour évaluer les contenus en cause, il en informe sans tarder les autorités compétentes ou l'organe compétent de l'Union, en indiquant les informations complémentaires ou les précisions dont il a besoin.

Article 6
Mesures proactives

1. Les fournisseurs de services d'hébergement prennent, [...] ***selon le risque et le niveau d'exposition aux contenus à caractère terroriste***, des mesures proactives pour protéger leurs services contre la diffusion de contenus à caractère terroriste. Ces mesures sont efficaces et proportionnées, compte tenu du risque et du niveau d'exposition aux contenus à caractère terroriste, des droits fondamentaux des utilisateurs et de l'importance fondamentale de la liberté d'expression et d'information dans une société ouverte et démocratique.

2. Lorsqu'elle a été informée conformément à l'article 4, paragraphe 9, l'autorité compétente visée à l'article 17, paragraphe 1, point c), demande au fournisseur de services d'hébergement de soumettre, dans les trois mois suivant la réception de la demande, et ensuite au moins une fois par an, un rapport sur les mesures proactives spécifiques qu'il a prises, y compris au moyen d'outils automatisés, en vue:
 - a) [...] de ***lutter efficacement contre la réapparition*** [...] de contenus qui ont été supprimés ou dont l'accès a été bloqué parce qu'ils sont considérés comme revêtant un caractère terroriste;

 - b) de détecter, d'identifier et de supprimer sans délai les contenus à caractère terroriste, ou de bloquer l'accès à ceux-ci.

Les demandes à cet effet sont adressées au siège principal du fournisseur de services d'hébergement ou au représentant légal désigné par ce dernier.

Les rapports contiennent toutes les informations pertinentes permettant à l'autorité compétente visée à l'article 17, paragraphe 1, point c), de déterminer si les mesures proactives sont efficaces et proportionnées, notamment en vue d'évaluer le fonctionnement des outils automatisés utilisés ainsi que la surveillance humaine et les mécanismes de vérification employés.

3. Si l'autorité compétente visée à l'article 17, paragraphe 1, point c), estime que les mesures proactives prises et communiquées en vertu du paragraphe 2 sont insuffisantes pour atténuer et gérer le risque et le niveau d'exposition, elle peut demander au fournisseur de services d'hébergement de prendre des mesures proactives spécifiques supplémentaires. À cette fin, le fournisseur de services d'hébergement coopère avec l'autorité compétente visée à l'article 17, paragraphe 1, point c), en vue d'identifier les mesures spécifiques que le fournisseur de services d'hébergement met en place, de fixer des objectifs clés et des critères de référence et de fixer des calendriers de mise en œuvre.
4. Si aucun accord ne peut être obtenu dans le délai des trois mois à compter de la demande visée au paragraphe 3, l'autorité compétente visée à l'article 17, paragraphe 1, point c), peut arrêter une décision imposant des mesures supplémentaires nécessaires et des mesures proactives proportionnées. Cette décision tient compte, en particulier, des capacités économiques du fournisseur de services d'hébergement, de l'incidence des mesures concernées sur les droits fondamentaux des utilisateurs et de l'importance fondamentale de la liberté d'expression et d'information. ***Il est laissé à la discrétion de l'autorité compétente visée à l'article 17, paragraphe 1, point c), de décider de la nature et de la portée des mesures proactives, conformément à l'objectif du présent règlement.*** La décision est adressée au siège principal du fournisseur de services d'hébergement ou au représentant légal désigné par ce dernier. Le fournisseur de services d'hébergement rend régulièrement compte de la mise en œuvre des mesures, conformément aux indications de l'autorité compétente visée à l'article 17, paragraphe 1, point c).
5. Le fournisseur de services d'hébergement peut, à tout moment, solliciter un réexamen à l'autorité compétente visée à l'article 17, paragraphe 1, point c), et, le cas échéant, l'annulation d'une demande ou d'une décision visée, respectivement, aux paragraphes 2, 3 et 4. L'autorité compétente prend une décision motivée dans un délai raisonnable après avoir reçu la demande du fournisseur de services d'hébergement.

Article 7

Conservation des contenus et des données connexes

1. Les fournisseurs de services d'hébergement conservent les contenus à caractère terroriste qui ont été supprimés ou dont l'accès a été bloqué à la suite d'une injonction de suppression, d'un signalement ou de mesures proactives prises en application des articles 4, 5 et 6, ainsi que les données connexes dont la suppression est intervenue parallèlement à celle des contenus incriminés, [...] qui sont nécessaires aux fins:
 - a) des procédures de réexamen administratif ou de contrôle juridictionnel,
 - b) de la prévention et de la détection d'infractions en relation avec le terrorisme ainsi que des enquêtes ou des poursuites y afférentes.
2. Les contenus à caractère terroriste et les données connexes visées au paragraphe 1 sont conservés pendant six mois. À la demande de l'autorité compétente ou d'un tribunal, les contenus à caractère terroriste sont conservés pendant une période plus longue, aussi longtemps que nécessaire, aux fins des procédures de réexamen administratif ou de contrôle juridictionnel en cours visées au paragraphe 1, point a).
3. Les fournisseurs de services d'hébergement veillent à ce que les contenus à caractère terroriste et les données connexes conservés conformément aux paragraphes 1 et 2 fassent l'objet de garanties techniques et organisationnelles appropriées.

Ces mesures garantissent que les contenus terroristes et données connexes ne sont accessibles et traités qu'aux fins visées au paragraphe 1 et que la protection des données à caractère personnel concernées bénéficie du plus haut niveau de sécurité. Les fournisseurs de services d'hébergement révisent et actualisent ces garanties autant que de besoin.

SECTION III GARANTIES ET RESPONSABILITÉS

Article 8

Obligations en matière de transparence

1. Les fournisseurs de services d'hébergement définissent, dans leurs conditions commerciales, leur politique de prévention de la diffusion de contenus à caractère terroriste, et y joignent, le cas échéant, une explication pertinente du fonctionnement des mesures proactives, y compris le recours à des outils automatisés.
2. Les fournisseurs de services d'hébergement, [...] qui sont **exposés aux contenus terroristes**, publient des rapports annuels sur la transparence indiquant les mesures prises en matière de diffusion des contenus à caractère terroriste.
3. Les rapports annuels sur la transparence comprennent au moins des informations sur:
 - a) les mesures prises par le fournisseur de services d'hébergement en ce qui concerne la détection, l'identification et la suppression des contenus à caractère terroriste;
 - b) les mesures prises par le fournisseur de services d'hébergement pour **lutter efficacement contre** [...] la ré[...] **apparition** de contenus qui ont été supprimés ou dont l'accès a été bloqué parce qu'ils sont considérés comme revêtant un caractère terroriste;
 - c) le nombre d'articles à caractère terroriste qui ont été supprimés ou dont l'accès a été bloqué à la suite, respectivement, d'injonctions de suppression, de signalements ou de mesures proactives;
 - d) et un récapitulatif des procédures de réclamation et de leur aboutissement.

Article 9

Garanties concernant l'utilisation et la mise en œuvre de mesures proactives

1. Lorsque des fournisseurs de services d'hébergement recourent à des procédés automatisés, conformément au présent règlement, pour les contenus qu'ils stockent, ils prévoient des garanties efficaces et adéquates pour assurer l'exactitude et le bien-fondé des décisions prises au sujet de ces contenus, en particulier les décisions relatives à la suppression de contenus considérés comme terroristes ou au blocage de l'accès à ces derniers.

2. Ces garanties consistent notamment 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 nécessaire pour déterminer si les contenus doivent être considérés comme revêtant ou non un caractère terroriste.

Article 10

Dispositifs de réclamation

1. Les fournisseurs de services d'hébergement établissent des mécanismes efficaces et accessibles permettant aux fournisseurs de contenus dont les contenus ont été supprimés ou dont l'accès a été bloqué à la suite d'un signalement en vertu de l'article 5 ou de mesures proactives en vertu de l'article 6 d'introduire une réclamation contre l'action du fournisseur de services d'hébergement et de demander le rétablissement des contenus concernés.
2. Les fournisseurs de services d'hébergement examinent dans les meilleurs délais toute réclamation qu'ils reçoivent et rétablissent sans tarder les contenus en cause dès lors qu'il était injustifié de les supprimer ou d'en bloquer l'accès. Ils informent l'auteur de la réclamation des conclusions de leur examen.

Article 11

Informations à l'attention du fournisseur de contenus

1. Lorsque des fournisseurs de services d'hébergement suppriment des contenus à caractère terroriste ou bloquent l'accès à ceux-ci, ils mettent à la disposition du fournisseur de contenus concerné des informations relatives à la suppression de ces contenus ou au blocage de l'accès à ceux-ci.
2. Sur demande du fournisseur de contenus, le fournisseur de services d'hébergement lui communique les motifs de la suppression de ses contenus ou du blocage de l'accès à ceux-ci, et l'informe de ses possibilités de recours.

3. L'obligation prévue aux paragraphes 1 et 2 ne s'applique pas lorsque l'autorité compétente décide que les motifs correspondants ne doivent pas être divulgués, pour des raisons de sécurité publique telles que la prévention et la détection d'infractions en relation avec le terrorisme ainsi que les enquêtes ou les poursuites y afférentes, et ce aussi longtemps que nécessaire, sans [...] pour autant excéder [...] **six** semaines à compter de la décision de suppression ou de blocage. ***Cette période peut être prolongée une fois pour une nouvelle période de six semaines, lorsque cela se justifie.*** En pareil cas, le fournisseur de services d'hébergement ne divulgue aucune information sur la suppression des contenus à caractère terroriste ou le blocage de l'accès à ceux-ci.

SECTION IV

Coopération entre les autorités compétentes, les organes de l'Union et les fournisseurs de services d'hébergement

Article 12

Capacités des autorités compétentes

Les États membres veillent à ce que leurs autorités compétentes disposent de la capacité nécessaire et de ressources suffisantes pour atteindre les objectifs et remplir les obligations qui leur incombent en vertu du présent règlement.

Article 13

*Coopération entre les fournisseurs de services d'hébergement, les autorités compétentes et, le cas échéant, [...] les organes **compétents** de l'Union*

1. Les autorités compétentes des États membres échangent des informations, se coordonnent et collaborent les unes avec les autres et, le cas échéant, avec [...] les organes **compétents** de l'Union, tels qu'Europol, en ce qui concerne les décisions de suppression de contenus et les signalements, de manière à éviter les doubles emplois, à renforcer la coordination et à éviter toute interférence avec les enquêtes en cours dans les différents États membres.
2. Les autorités compétentes des États membres échangent des informations, se coordonnent et collaborent avec l'autorité compétente visée à l'article 17, paragraphe 1, points c) et d), en ce qui concerne les mesures prises en vertu de l'article 6 et les mesures d'exécution prises en vertu de l'article 18. Les États membres veillent à ce que l'autorité compétente visée à l'article 17, paragraphe 1, points c) et d), soit en possession de toutes les informations pertinentes. À cette fin, les États membres prévoient les canaux ou mécanismes de communication appropriés permettant de faire en sorte que les informations pertinentes soient partagées en temps utile.

3. ***Aux fins de la mise en œuvre effective du présent règlement ainsi que pour éviter les doubles emplois***, les États membres et les fournisseurs de services d'hébergement peuvent choisir d'utiliser des outils dédiés, y compris [...] ceux établis par [...] les organes ***compétents*** de l'Union tels qu'Europol, afin de faciliter en particulier:
- a) le traitement des données et le retour d'information relatifs aux décisions de suppression de contenus, en application de l'article 4;
 - b) le traitement des données et le retour d'information relatifs aux signalements, en application de l'article 5;
 - c) la coopération visant à identifier et à mettre en œuvre des mesures proactives en application de l'article 6.
4. Lorsqu'un fournisseur de services d'hébergement a connaissance de tout élément de preuve relatif à une infraction à caractère terroriste, il en informe sans délai les autorités compétentes pour les enquêtes et les poursuites en matière d'infractions pénales dans l'État membre concerné ***(ou les États membres concernés)*** [...]. ***Lorsqu'il est impossible d'identifier l'État membre ou les États membres concernés*** [...], le fournisseur de services d'hébergement [...] ***notifie le point de contact, tel que visé à l'article 14, paragraphe 3, dans l'État membre où il a son établissement principal ou dispose d'un représentant légal, et transmet également*** ces informations à Europol, qui leur réservera un suivi approprié.

Article 14

Points de contact

1. Les fournisseurs de services d'hébergement établissent un point de contact permettant de recevoir des injonctions de suppression et des signalements par voie électronique et d'en assurer un traitement rapide, conformément aux articles 4 et 5. Ils font en sorte que cette information soit accessible au public.

2. Les informations visées au paragraphe 1 précisent la ou les langues officielles de l'Union, visées au règlement (CE) n° 1/58, dans lesquelles il est possible de s'adresser au point de contact et dans lesquelles se déroulent les autres échanges concernant les injonctions de suppression et les signalements, conformément aux articles 4 et 5. Ces langues comprennent au moins une des langues officielles de l'État membre dans lequel le fournisseur de services d'hébergement a son établissement principal ou dans lequel réside ou est établi son représentant légal conformément à l'article 16.
3. Les États membres établissent un point de contact pour traiter les demandes de précisions et de retour d'information en rapport avec les injonctions de suppression et les signalements émis par leurs soins. Les informations relatives à ce point de contact sont rendues publiques.

SECTION V

MISE EN ŒUVRE ET APPLICATION

Article 15

Compétence

1. L'État membre dans lequel est situé l'établissement principal du fournisseur de services d'hébergement est compétent aux fins des articles 6, 18 et 21. Tout fournisseur de services d'hébergement dont l'établissement principal n'est pas situé dans un des États membres est considéré comme relevant de la juridiction de l'État membre dans lequel le représentant légal visé à l'article 16 réside ou est établi. ***Tout État membre est compétent aux fins des articles 4 et 5, quel que soit le lieu où le fournisseur de services d'hébergement a son établissement principal ou dans lequel il a désigné un représentant légal.***
2. Si le fournisseur de services d'hébergement n'a pas désigné de représentant légal, tous les États membres sont compétents. ***Lorsqu'un État membre décide d'exercer sa compétence, il en informe tous les autres États membres.***

[...] [...]

[...]Article 16
Représentant légal

1. Tout fournisseur de services d'hébergement qui n'est pas établi dans l'Union mais offre des services dans l'Union désigne, par écrit, une personne physique ou morale comme son représentant légal dans l'Union, pour la réception, la mise en œuvre et l'exécution des injonctions de suppression, des signalements, des demandes et des décisions émis par les autorités compétentes sur la base du présent règlement. Le représentant légal réside ou est établi dans un des États membres où le fournisseur de services d'hébergement offre ses prestations.
2. Le représentant légal est chargé, au nom du fournisseur de services d'hébergement concerné, de recevoir, de mettre en œuvre et de faire exécuter les injonctions de suppression, les signalements, les demandes et des décisions visés au paragraphe 1. Les fournisseurs de services d'hébergement donnent à leur représentant légal les pouvoirs et les ressources nécessaires pour coopérer avec les autorités compétentes et se conformer auxdites décisions et injonctions.
3. Le représentant légal désigné peut être tenu pour responsable du non-respect des obligations au titre du présent règlement, sans préjudice de la responsabilité du fournisseur de services d'hébergement et des actions en justice susceptibles d'être intentées contre lui.
4. Le fournisseur de services d'hébergement informe de la désignation du représentant légal l'autorité compétente visée à l'article 17, paragraphe 1, point d), de l'État membre dans lequel ledit représentant légal réside ou est établi. Les informations relatives au représentant légal sont mises à la disposition du public.

SECTION VI
DISPOSITIONS FINALES

Article 17

Désignation des autorités compétentes

1. Les États membres désignent l'autorité ou les autorités compétentes chargées:
 - a) d'émettre les injonctions de suppression conformément à l'article 4;
 - b) de détecter et d'identifier les contenus à caractère terroriste et de les signaler aux fournisseurs de services d'hébergement, en application de l'article 5;
 - c) de superviser la mise en œuvre des mesures proactives en application de l'article 6;
 - d) de faire respecter les obligations prévues au présent règlement sous peine de sanctions, en application de l'article 18.

2. Le [***douze*** [...] *mois après l'entrée en vigueur du présent règlement*] au plus tard, les États membres notifient à la Commission ***l'autorité ou*** les autorités compétentes visées au paragraphe 1. La Commission publie cette notification et toute modification y afférente au *Journal officiel de l'Union européenne*.

Article 18

Sanctions

1. Les États membres déterminent le régime des sanctions applicables en cas de manquement aux obligations qui incombent aux fournisseurs de services d'hébergement en application du présent règlement et prennent toutes les mesures nécessaires pour en assurer l'exécution. Ces sanctions concernent exclusivement les manquements aux obligations découlant:
 - a) de l'article 3, paragraphe 2 (conditions commerciales des fournisseurs de services d'hébergement);
 - b) de l'article 4, paragraphes 2 et 6 (mise en œuvre des injonctions de suppression et retour d'informations y afférent);

- c) de l'article 5, paragraphes 5 et 6 (évaluation des signalements et retour d'informations y afférent);
 - d) de l'article 6, paragraphes 2 et 4 (rapports relatifs aux mesures proactives et adoption de mesures à la suite de décisions imposant des mesures proactives spécifiques);
 - e) de l'article 7 (conservation des données);
 - f) de l'article 8 (transparence);
 - g) de l'article 9 (garanties liées aux mesures proactives);
 - h) de l'article 10 (procédures de réclamation);
 - i) de l'article 11 (information des fournisseurs de contenus);
 - j) de l'article 13, paragraphe 4 (informations liées aux preuves relatives aux infractions terroristes);
 - k) de l'article 14, paragraphe 1 (points de contact);
 - l) de l'article 16 (désignation d'un représentant légal).
2. Les sanctions prévues sont effectives, proportionnées et dissuasives. Les États membres informent la Commission, au plus tard le... [[...] *mois après la date d'entrée en vigueur du présent règlement*], des règles et mesures adoptées à cet égard ainsi que, sans retard, de toute modification qui y serait apportée ultérieurement.
3. Les États membres veillent à ce que les autorités compétentes, lorsqu'elles déterminent le type et le niveau des sanctions, tiennent compte de toutes les circonstances pertinentes, et notamment:
- a) de la nature, de la gravité et de la durée de l'infraction;
 - b) de l'origine de l'infraction (acte intentionnel ou négligence);
 - c) des infractions commises précédemment par la personne morale **ou physique** tenue pour responsable;

- d) de la solidité financière de la personne morale **ou physique** tenue pour responsable;
 - e) du niveau de coopération du fournisseur de services d'hébergement avec les autorités compétentes.
4. Les États membres veillent à ce que le non-respect systématique des obligations prévues à l'article 4, paragraphe 2, soit passible de sanctions financières pouvant atteindre jusqu'à 4 % du chiffre d'affaires global du fournisseur de services d'hébergement pour l'exercice précédent.

Article 19

Exigences techniques et modification des modèles à utiliser pour les injonctions de suppression

1. La Commission est habilitée à adopter des actes délégués conformément à l'article 20 afin de compléter le présent règlement par des exigences techniques concernant les moyens électroniques à utiliser par les autorités compétentes pour la transmission des injonctions de suppression.
2. La Commission est ainsi habilitée à adopter des actes délégués pour modifier les annexes I, II et III afin de réagir efficacement s'il devenait nécessaire d'améliorer le contenu des formulaires à utiliser pour les injonctions de suppression ou pour fournir des informations sur l'impossibilité d'exécuter une injonction de suppression.

Article 20

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.
2. Le pouvoir d'adopter les actes délégués visés à l'article 19 est conféré à la Commission pour une durée indéterminée à compter du [*date d'application du présent règlement*].

3. La délégation de pouvoir visée à l'article 19 peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est spécifiée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.
4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel "Mieux légiférer" du 13 avril 2016.
5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie simultanément au Parlement européen et au Conseil.
6. Un acte délégué adopté en vertu de l'article 19 n'entre en vigueur que s'il n'a donné lieu à aucune objection du Parlement européen ou du Conseil dans un délai de deux mois à compter de sa notification au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 21

Suivi

1. Les États membres recueillent, auprès de leurs autorités compétentes et des fournisseurs de services d'hébergement relevant de leur juridiction, des informations sur les mesures qu'ils ont prises conformément au présent règlement et les communiquent à la Commission pour le [31 mars] de chaque année. Il s'agit notamment:
 - a) d'informations sur le nombre d'injonctions de suppression et de signalements émis et le nombre d'articles à caractère terroriste qui ont été supprimés ou dont l'accès a été bloqué, assorti de l'indication des délais correspondants, conformément aux articles 4 et 5;

- b) des informations sur les mesures proactives spécifiques prises en application de l'article 6, et notamment de l'indication de la quantité de contenus à caractère terroriste qui ont été supprimés ou dont l'accès été bloqué, ainsi que les délais correspondants;
- c) des informations sur le nombre de procédures de réclamation ouvertes et sur les mesures prises par les fournisseurs de services d'hébergement en application de l'article 10;
- d) des informations sur le nombre de procédures de recours engagées et sur les décisions prises par l'autorité compétente conformément au droit national.

2. Au plus tard le [*un an à compter de la date d'application du présent règlement*], la Commission établit un programme détaillé pour le suivi des réalisations, des résultats et des incidences du présent règlement. Ce programme de suivi définit les indicateurs et les moyens à utiliser, ainsi que les intervalles à appliquer pour recueillir les données et d'autres éléments de preuve nécessaires. Il précise les mesures que la Commission et les États membres doivent prendre en vue de recueillir et d'analyser les données et autres éléments permettant de suivre l'état d'avancement et d'évaluer le présent règlement, en application de l'article 23.

Article 22

Rapport de mise en œuvre

Le ... [*deux ans après l'entrée en vigueur du présent règlement*] au plus tard, la Commission présente au Parlement européen et au Conseil un rapport sur l'application du présent règlement. Le rapport de la Commission prend en compte les informations relatives au suivi recueillies conformément à l'article 21 et les informations résultant des obligations de transparence recueillies conformément à l'article 8. Les États membres fournissent à la Commission les informations nécessaires à l'élaboration de ce rapport.

Article 23

Évaluation

Dans un délai minimal de [*trois ans à compter de la date d'application du présent règlement*], la Commission procède à une évaluation du présent règlement et présente au Parlement européen et au Conseil un rapport sur son application, qui couvre notamment le fonctionnement et l'efficacité des mécanismes relatifs aux garanties. Le cas échéant, le rapport est accompagné de propositions législatives. Les États membres fournissent à la Commission les informations nécessaires à l'élaboration de ce rapport.

Article 24

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il s'applique à compter du [*douze [...] mois après son entrée en vigueur*].

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le

Par le Parlement européen
Le président

Par le Conseil
Le président