Retrait des contenus terroristes en ligne

Delhaise, Elise

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2022

Document Version
le PDF de l'éditeur

Retrait des contenus terroristes en ligne : l'Union européenne lutte contre la propagande terroriste virtuelle

Elise Delhaise

Le Parlement européen et le Conseil ont adopté le 29 avril 2021 un règlement visant à lutter contre la « propagande » terroriste en ligne. La présente contribution a pour objectif de délimiter le champ d'application de ce règlement ainsi que son objet.

The European Parliament and the Council adopted a Regulation tofight against the dissemination of terrorist content online on April 29, 2021. The Regulation's scope and object will be briefly exposed in this text.

INTRODUCTION[1]

Le Parlement européen et le Conseil ont adopté le 29 avril 2021 un règlement[2] visant à lutter contre la « propagande » terroriste[3] en ligne. La présente contribution poursuit un triple objectif :

- présenter le règlement, son champ d'application et les différentes obligations des acteurs (I. Le règlement (UE) 2021/784) ;
- analyser les systèmes mis en œuvre au niveau national (II. Les mises en œuvre nationales : les exemples français et belge) ;
- proposer une analyse critique de plusieurs principes transversaux du règlement (III. Les contenus terroristes : du texte vague du règlement aux incidences pratiques alarmantes).

I. LE RÈGLEMENT (UE) 2021/784

Cette première partie est consacrée à la présentation du règlement. Dans cette optique, nous analyserons successivement sa *ratio legis* (A), son champ d'application (B), le retrait et le blocage des contenus terroristes (C), les autres obligations des fournisseurs de services d'hébergement (D) et les contrôles et sanctions (E).

A. La *ratio legis*

Internet permet d'atteindre un large public, à coût minime et les criminels l'ont bien compris, notamment en matière de terrorisme. En effet, les contenus terroristes partagés en ligne contribuent à recruter des sympathisants ou à préparer la commission d'infractions[4].

[1] Nous tenons à remercier chaleureusement Nathalie Colette-Basecqz pour sa relecture ainsi que Manon Knockaert, Amélie Lachapelle, Michaël Lognoul et François Xavier pour leurs éclairages respectifs.

[2] Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, *J.O.U.E.*, 17 mai 2021, L 172/79.

[3] Règlement (UE) 2021/784 précité, considérant 11.

[4] Proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffu-

L'Union européenne est préoccupée par cette problématique[5] et a déjà mobilisé divers mécanismes afin de lutter contre celle-ci. Nous pouvons notamment citer :

- la directive sur le commerce électronique devant « constituer la base adéquate pour l'élaboration de mécanismes rapides et fiables permettant de retirer les informations illicites et de rendre l'accès à celles-ci impossible »[6] ;
- le forum de l'UE sur l'Internet de 2015 encourageant « les États membres et les fournisseurs de services d'hébergement à coopérer volontairement et à prendre des mesures afin de réduire l'accessibilité des contenus à caractère terroriste en ligne et de donner aux partenaires de la société civile les moyens de multiplier les contre-discours efficaces en ligne »[7] ;
- le Code de conduite sur la lutte contre les discours haineux illégaux en ligne élaboré en juin 2016 par la Commission européenne, Facebook, Microsoft, Twitter et YouTube avec pour objectif de baliser leurs propres activités et partager les bonnes pratiques avec d'autres entreprises, plateformes et réseaux sociaux[8] ;
- la recommandation (UE) 2018/334 de la Commission du 1er mars 2018 sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne[9]. Celle-ci définit notamment les contenus illicites[10] et propose des mesures spécifiques en matière de contenus terroristes[11].

Néanmoins, ces efforts sont considérés comme insuffisants par l'Union européenne, rendant l'adoption d'un règlement indispensable afin d'agir face aux contenus à caractère terroriste en ligne « en imposant un ensemble minimal d'obligations de vigilance aux fournisseurs de services d'hébergement, dont certaines règles et contraintes spécifiques, ainsi que des obligations aux États membres »[12].

B. Le champ d'application du règlement (article 1er)

Le règlement vise à établir des règles uniformes afin de lutter contre la propagande terroriste, en poursuivant un double objectif :

- préciser les devoirs de vigilance des fournisseurs de services d'hébergement afin de lutter contre la diffusion des contenus au public, voire de les retirer ou d'en bloquer l'accès ;
- déterminer les mesures à prendre par les États pour identifier les contenus terroristes, veiller à leur retrait et faciliter la collaboration entre les différents acteurs impliqués.

Comme nous venons de le souligner, ce règlement est exclusivement consacré à la problé-

sion de contenus à caractère terroriste en ligne du 12 septembre 2018, COM(2018) 640 final, p. 1.

5 Règlement (UE) 2021/784 précité, considérant 4).

6 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 »), *J.O.C.E.*, 17 juillet 2000, L 178/1, considérant 40.

7 Proposition COM(2018) 640 final de règlement précitée, p. 1.

8 Code of conduct on countering illegal hate speech online, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

9 Recommandation (UE) 2018/334 de la Commission du 1er mars 2018 sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne, *J.O.U.E.*, 6 mars 2018, L 63/50.

10 « toute information contraire au droit de l'Union ou au droit de l'État membre concerné ». Recommandation (UE) 2018/334 précitée, § 4, b).

11 Recommandation (UE) 2018/334 précitée, Chapitre III.

12 Proposition COM(2018) 640 final de règlement précitée, p. 2.

matique des contenus terroristes. Néanmoins, Internet est utilisé pour mener toute une série d'autres activités illicites. Par conséquent, d'autres instruments européens sont applicables pour lutter contre, par exemple, la diffusion de matériel pédopornographique[13] ou de discours de haine illégaux[14]. Face à cette problématique multiforme, l'Union européenne prévoit d'adopter un cadre général de lutte contre la diffusion de contenus illicites[15], sans toutefois affecter l'application du règlement 2021/784 consacré aux contenus terroristes, le qualifiant de *lex specialis*[16].

Détaillons à présent la notion centrale de contenus terroristes (1) et présentons les divers acteurs (2) mobilisés dans le cadre de la lutte contre la propagande terroriste en ligne.

1. *Les contenus terroristes et leur diffusion au public*

Le règlement 2021/784 vise à lutter contre la propagande terroriste[17] en ligne. Il convient donc de revenir sur les notions de « contenus terroristes » et de « diffusion au public ».

Tout d'abord, un contenu terroriste est « le matériel qui incite à ou sollicite une personne pour commettre une infraction terroriste visée à l'article 3, §1er, points a) à i) de la Directive (UE) 2017/541, qui sollicite une (plusieurs) personne(s) pour participer aux activités d'un groupe terroriste, fournit des instructions concernant la fabrication ou l'utilisation d'explosifs, d'armes à feu ou d'autres armes, ou de substances nocives ou dangereuses, ou concernant d'autres méthodes ou techniques spécifiques afin de commettre ou contribuer à commettre une infraction terroriste ou qui constitue une menace quant à la commission d'une infraction terroriste »[18]. Précisons que le règlement ne couvre pas uniquement les vidéos, mais aussi les images et les textes[19].

Il s'agit donc d'un contenu diffusé en amont de la commission de l'infraction terroriste au sens strict, définie comme l'un des comportements visés à l'article 3 de la directive (UE) 2017/541 ou de la participation aux activités d'un groupe terroriste. En effet, ce contenu vise à inciter, à solliciter ou à préparer à la commission de l'infraction terroriste au sens strict. Il s'agit dès lors sans aucun doute d'un instrument à visée préventive et anticipative.

Ensuite, les contenus terroristes, pour être considérés comme de la propagande, doivent être diffusés au public, à savoir mis « à la disposition d'un nombre potentiellement illimité de personnes, à la demande d'un fournisseur de contenus »[20].

Précisons enfin que le contenu diffusé « à des fins éducatives, journalistiques, artistiques ou de recherche, ou à des fins de prévention ou de lutte contre le terrorisme, y compris le matériel qui représente l'expression d'opinions polémiques ou controversées dans le cadre du débat public, n'est pas considéré comme étant un contenu à

13 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, *J.O.U.E.*, 17 décembre 2011, L 335/1.

14 Décision-cadre 2008/913/JAI du Conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal, *J.O.U.E.*, 6 décembre 2008, L 325/55.

15 Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, COM(2020) 825 final, art. 8.

16 Proposition COM(2020) 825 final précitée, pp. 5 et 21.

17 Règlement (UE) 2021/784 précité, considérant 11.

18 Règlement (UE) 2021/784 précité, art. 2, 7).

19 Proposition COM(2018) 640 final de règlement précitée, p. 4.

20 Règlement (UE) 2021/784 précité, art. 2, 3).

caractère terroriste »[21]. Il convient donc d'analyser le véritable objectif de la diffusion avant de qualifier celle-ci de diffusion terroriste.

2. *Le fournisseur de contenus, le fournisseur de services d'hébergement et l'autorité compétente*

Trois acteurs principaux sont impliqués dans la diffusion de contenus terroristes et la lutte contre celle-ci :

- le fournisseur de contenus lui-même ;
- le fournisseur de services d'hébergement ;
- l'autorité compétente.

Tout d'abord, le fournisseur de contenus est défini par le règlement comme « un utilisateur qui a fourni des informations qui sont stockées, ou qui l'ont été, et diffusées au public par un fournisseur de services d'hébergement ». Dans le cadre du présent règlement, ce sont des contenus à caractère terroriste qui sont fournis par le fournisseur de contenus. Précisons que le règlement ne contient aucune disposition pénale incriminant cette fourniture de contenu. En effet, les infractions terroristes sont incriminées par d'autres instruments européens. Ainsi, la fourniture de contenus pourrait être qualifiée d'infraction de provocation publique à commettre une infraction terroriste[22], de recrutement pour le terrorisme[23] ou de dispense d'un entraînement au terrorisme[24]. Par conséquent, seul le sort à réserver aux contenus terroristes est traité par le règlement analysé, la poursuite pénale du fournisseur étant assurée par d'autres canaux.

Ensuite, le fournisseur de services d'hébergement doit s'entendre comme « un fournisseur de services[25] qui consistent à stocker des informations fournies par un fournisseur de contenus à la demande de celui-ci ». Le règlement va plus loin que la directive 2010/13/UE[26], telle que modifiée par la directive (UE) 2018/1808[27], en ce qu'il ne s'applique pas uniquement aux plateformes de partage de vidéos, mais à tous les types de fournisseurs de services d'hébergement[28].

D'un point de vue territorial, ce sont les fournisseurs de services d'hébergement qui proposent des services dans l'Union européenne qui sont visés, à savoir ceux qui « permett[ent] à des personnes physiques ou morales dans un ou plusieurs États membres d'utiliser les services d'un fournisseur de services d'hébergement qui a un lien étroit avec cet État membre ou ces États membres »[29], peu importe leur lieu d'établissement principal. Précisons néan-

21 Règlement (UE) 2021/784 précité, art. 1er, § 3.

22 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, *J.O.U.E.*, 31 mars 2017, L 88/6, art. 5.

23 Directive (UE) 2017/541 précitée, art. 6.

24 Directive (UE) 2017/541 précitée, art. 7.

25 « tou[s] service[s] de la société de l'information, c'est-à-dire tou[s] service[s] presté[s] normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services ». Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.U.E.*, 17 septembre 2015, L 241/1, art. 1er, b).

26 Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels »), *J.O.U.E.*, 14 avril 2010, L 95/1.

27 Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018, modifiant la directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché, *J.O.U.E.*, 28 novembre 2018, L 303/69.

28 Proposition COM(2018) 640 final de règlement précitée, p. 4.

29 Règlement (UE) 2021/784 précité, art. 2, § 4.

moins qu'un « lien étroit »[30] doit exister entre le fournisseur d'hébergement et un ou plusieurs États membres. Ce règlement ne concerne néanmoins pas tous les fournisseurs de tous les services. En effet, seuls sont visés les fournisseurs diffusant des informations au public[31].

Enfin, chaque État membre est tenu de désigner une ou plusieurs autorités compétentes afin d'exercer les compétences visées à l'article 12, § 1er, du règlement. Celui-ci reste muet quant au profil de cette autorité (autorité judiciaire ? administrative ? policière ?), dont l'identité devra être communiquée à la Commission européenne au plus tard le 7 juin 2022.

C. Le retrait ou le blocage de l'accès aux contenus terroristes

Le retrait ou le blocage de l'accès aux contenus terroristes est l'objectif principal du règlement. Pour y parvenir, une procédure en plusieurs étapes est d'application : émission d'une injonction de retrait par une autorité compétente (1), retrait ou blocage par le fournisseur de services d'hébergement (2), conservation des contenus (3) et information du fournisseur de contenus (4).

1. L'injonction de retrait (article 3, §§ 1 et 2, §§ 4 et 5 et article 4, §§ 1 et 2)

L'autorité compétente peut émettre une injonction de retrait à l'attention d'un fournisseur de services d'hébergement afin que celui-ci retire les contenus terroristes ou qu'il bloque l'accès à ces contenus. Cette injonction est adressée :

- à l'établissement principal du fournisseur de services d'hébergement ou à son représentant légal (dans le cas où le fournisseur de services a son établissement principal ou son représentant légal dans l'État membre de l'autorité compétente) ;
- à l'établissement principal du fournisseur de services d'hébergement ou à son représentant légal ainsi qu'une copie à l'autorité compétente de l'État membre dans lequel le fournisseur de services d'hébergement a son établissement principal ou dans lequel son représentant légal réside ou est établi (dans le cas d'une injonction de retrait transfrontière, cas où le fournisseur de services n'a pas son établissement principal ou n'a pas de représentant légal dans l'État membre de l'autorité compétente).

Le contenu de l'injonction de retrait est déterminé dans un modèle annexé au règlement (Annexe I). Elle doit notamment contenir une motivation suffisamment détaillée expliquant les raisons pour lesquelles le contenu est considéré comme étant un contenu à caractère terroriste, une URL exacte ainsi que les possibilités de recours.

La question de savoir comment et par qui les contenus terroristes seront identifiés n'est cependant pas traitée par le règlement. Comment l'autorité compétente va-t-elle avoir connaissance de l'existence de ces contenus ? Plusieurs méthodes peuvent être employées :

- dispositifs technologiques de prévention (paramètres automatisés, algorithmes, moteurs de recherche…)[32] ;

[30] « lien qu'un fournisseur de services d'hébergement a avec un ou plusieurs États membres, qui résulte soit de son établissement dans l'Union soit de critères factuels précis, tels que : a) avoir un nombre significatif d'utilisateurs de ses services dans un ou plusieurs États membres ; ou b) le ciblage de ses activités vers un ou plusieurs États membres ». Règlement (UE) 2021/784 précité, art. 2, § 5.

[31] Règlement (UE) 2021/784 précité, art. 1er, § 2.

[32] Avis du Comité économique et social européen sur la « Proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne » du 12 décembre 2018, *J.O.U.E.*, 22 mars 2019, C 110/67.

– facteur humain via des fonctions de médiation et d'intermédiation[33] ;
– dénonciation des associations, ONG, syndicats et usagers de la société civile[34].

Précisons enfin que s'il s'agit de la première injonction de retrait adressée à un fournisseur de services d'hébergement, l'autorité compétente est tenue de lui communiquer des informations sur les procédures et les délais applicables, au moins douze heures avant d'émettre l'injonction de retrait, sauf cas d'urgence dûment justifiés.

Si le fournisseur de services a reçu au moins deux injonctions de retrait au cours des douze derniers mois, il pourra être qualifié de fournisseur de services « exposé à des contenus terroristes », à la suite d'une décision de l'autorité compétente. Nous reviendrons ultérieurement sur ce statut de fournisseur de services « exposé à des contenus terroristes » et les obligations y attachées.

2. Le retrait ou le blocage (article 3, § 3 et §§ 6 à 8)

À la suite de la réception d'une injonction de retrait, le fournisseur de service est tenu de retirer les contenus ou de bloquer l'accès à ces contenus dès que possible, et, en tout état de cause, dans un délai d'une heure à compter de la réception de l'injonction de retrait. Il en informe ensuite l'autorité compétente, sans retard, et lui communique notamment la date et l'heure du retrait ou du blocage.

Nous verrons ultérieurement que le fournisseur de services est susceptible de se voir infliger une sanction s'il ne se conforme pas à l'injonction de retrait. Néanmoins, dans deux situations, le fournisseur de services peut avertir l'autorité compétente de l'impossibilité d'honorer son obligation de retrait ou de blocage :

– motifs de force majeure ou d'impossibilité de fait qui ne sont pas imputables au fournisseur de services, y compris pour des raisons techniques ou opérationnelles objectivement justifiables ;
– erreurs manifestes dans l'injonction de retrait ou celle-ci ne contient pas suffisamment d'informations pour en permettre l'exécution.

À la suite de cette information, le fournisseur de services devra se conformer à l'injonction de retrait dans un délai d'une heure, à compter soit de la disparition des motifs rendant impossible l'exécution de l'injonction, soit de la réception des éclaircissements demandés.

3. La conservation des contenus (article 6)

Lorsqu'un fournisseur de services a retiré un contenu terroriste ou a bloqué l'accès à ce contenu, il est tenu de le conserver. Cette conservation des contenus est assortie de plusieurs garanties :

– une garantie de nécessité : conservation du contenu nécessaire à des fins de procédures de réexamen administratif ou de contrôle juridictionnel, ou du traitement de réclamations au titre de l'article 10 ou à des fins de prévention et de détection d'infractions terroristes, ainsi que d'enquêtes ou de poursuites en la matière ;
– une garantie temporelle : contenu conservé pour une période de six mois. Cette période est renouvelable, seulement en cas de nécessité et aussi longtemps que nécessaire, aux fins de procédures de réexamen administratif ou de contrôle juridictionnel en cours ;
– des garanties techniques et organisationnelles : accès et traitement des données

[33] Avis du Comité économique et social européen précité, C 110/67.
[34] Avis du Comité économique et social européen précité, C 110/68-69.

uniquement à des fins de procédures de réexamen administratif ou de contrôle juridictionnel, ou du traitement de réclamations au titre de l'article 10 ou à des fins de prévention et de détection d'infractions terroristes, ainsi que d'enquêtes ou de poursuites en la matière et haut niveau de sécurité pour les données à caractère personnel.

4. L'information des fournisseurs de contenus (article 11)

À la suite du retrait d'un contenu terroriste ou du blocage de l'accès à ce contenu, le fournisseur de services est tenu de mettre à disposition du fournisseur de contenus certaines informations concernant le retrait ou le blocage. À la demande de ce dernier, il l'informe des motifs du retrait ou du blocage et des possibilités de recours. Le fournisseur peut également remettre une copie de l'injonction de retrait qui, pour rappel, contient ces informations.

Précisons cependant qu'en cas de motifs de sécurité publique, l'autorité compétente peut interdire la divulgation d'informations pour une période de six semaines, renouvelable aussi longtemps que nécessaire pour autant que la non-divulgation continue d'être justifiée et que celle-ci soit proportionnée.

D. Les autres obligations des fournisseurs de services d'hébergement

Outre l'obligation de se conformer à l'injonction de retrait et les obligations en découlant (conservation des contenus supprimés ou bloqués et information du fournisseur de contenus), le fournisseur de services se voit imposer plusieurs autres obligations. Nous pouvons distinguer plusieurs niveaux d'obligations :

- applicables à tous les fournisseurs de services (1) ;
- applicables aux fournisseurs de services dont l'établissement principal n'est pas situé dans l'Union européenne (2) ;
- applicables aux fournisseurs de services qui ont pris des mesures de lutte contre la diffusion de contenus à caractère terroriste ou auxquels il a été fait obligation de prendre des mesures en vertu du règlement au cours d'une année civile donnée (3) ;
- applicables aux fournisseurs de services « exposés à des contenus terroristes » (4).

1. Tous les fournisseurs de services

Trois obligations principales sont imposées à tous les fournisseurs de services d'hébergement.

Tout d'abord, leurs conditions générales doivent présenter clairement leur politique de lutte contre la diffusion des contenus à caractère terroriste. Ils peuvent également y joindre une explication détaillée du fonctionnement des mesures spécifiques, y compris, s'il y a lieu, du recours à des outils automatisés[35].

Ensuite, ils sont tenus de désigner un point de contact, chargé de la réception et du traitement des injonctions de retrait[36].

Enfin, afin d'assurer une bonne coopération entre les fournisseurs de services, les autorités compétentes et Europol, les fournisseurs de services sont obligés d'informer immédiatement les autorités compétentes pour les enquêtes et les poursuites en matière d'infractions pénales dans les États membres concernés dès qu'ils prennent connaissance d'un contenu à caractère terroriste présentant une menace imminente pour la vie[37].

2. Fournisseurs de services établis hors UE

En vertu de l'article 17, § 1er, du règlement, « [u]n fournisseur de services d'hébergement dont l'établissement principal n'est pas situé

35 Règlement (UE) 2021/784 précité, art. 7, § 1er.
36 Règlement (UE) 2021/784 précité, art. 15.
37 Règlement (UE) 2021/784 précité, art. 14, § 5.

dans l'Union désigne, par écrit, une personne physique ou morale en tant que son représentant légal dans l'Union aux fins de la réception, du respect et de l'exécution des injonctions de retrait et des décisions rendues par les autorités compétentes ».

3. Fournisseurs de services ayant pris des mesures de lutte ou auxquels il a été fait obligation de prendre des mesures

Ces fournisseurs de services doivent mettre à la disposition du public un rapport de transparence sur les mesures prises[38]. Ce rapport doit contenir un certain nombre d'indications, visées à l'article 7, § 3, du règlement, dont, notamment, les mesures prises et le nombre d'éléments de contenus terroristes retirés ou bloqués.

4. Fournisseurs de services « exposés à des contenus terroristes »

Nous avons précédemment évoqué le statut de fournisseur de services « exposé à des contenus terroristes ». Un fournisseur de services peut être qualifié comme tel à la suite d'une décision prise par l'autorité compétente et notifiée au fournisseur de services constatant l'exposition à des contenus terroristes. Pour apprécier cette exposition, l'autorité compétente se fonde sur des éléments objectifs, comme le nombre d'injonctions de retrait reçues par le fournisseur de services[39].

Ce statut de fournisseur « exposé à des contenus terroristes » implique le respect de trois obligations supplémentaires :

– inscription dans les conditions générales et application de dispositions visant à lutter contre l'utilisation abusive de ses services pour diffuser au public des contenus à caractère terroriste[40] ;
– prise de mesures efficaces, ciblées, proportionnées, tenant compte des droits et de l'intérêt légitime des utilisateurs et appliquées avec diligence et de façon non discriminatoire[41], pour protéger ses services contre la diffusion au public de contenus à caractère terroriste[42]. Sont citées, par exemple, des mesures techniques et opérationnelles ou des mécanismes de sensibilisation ;
– communication d'un rapport relatif aux mesures prises à l'autorité compétente[43].

E. Contrôles et sanctions

Nous avons pu le constater, les différents acteurs sont tenus de respecter de nombreuses obligations, dont la violation de certaines doit entraîner une sanction (2). Néanmoins, revenons dans un premier temps sur les mécanismes de contrôle prévus par le règlement afin que les injonctions de retrait soient conformes au règlement et aux libertés et droits fondamentaux garantis par la Charte et que les fournisseurs de services et de contenus puissent s'opposer à une décision de retrait ou de blocage (1).

1. Contrôles

a. L'examen approfondi de l'injonction de retrait (article 4, §§ 3 à 7)

Une autorité compétente d'un État a le droit d'adresser une injonction de retrait à un fournisseur de services dont l'établissement principal est situé dans un autre État. Il s'agit d'un cas d'injonction transfrontière. Par conséquent, comme le souligne la Ligue des droits humains,

38 Règlement (UE) 2021/784 précité, art. 7, §§ 2-3.
39 Règlement (UE) 2021/784 précité, art. 5, § 4.
40 Règlement (UE) 2021/784 précité, art. 5, § 1er.
41 Règlement (UE) 2021/784 précité, art. 5, § 3.
42 Règlement (UE) 2021/784 précité, art. 5, § 2.
43 Règlement (UE) 2021/784 précité, art. 5, § 5.

un État pratiquant la censure et violant certains droits fondamentaux comme la liberté d'expression pourrait étendre cette censure et ces violations à d'autres États par le biais de ces injonctions transfrontières[44]. Le règlement prévoit donc un contrôle par l'autorité compétente de l'État du fournisseur de services via un examen approfondi de l'injonction de retrait.

L'examen approfondi vise à déterminer si elle viole gravement ou manifestement le règlement ou les libertés et droits fondamentaux garantis par la Charte et a lieu :

- soit à l'initiative de l'autorité compétente de l'État où le fournisseur de services a son établissement principal, dans un délai de 72 heures à compter de la réception de la copie de l'injonction de retrait ;
- soit à la demande du fournisseur de services, dans un délai de 48 heures à compter de la réception de l'injonction de retrait ;
- soit à la demande du fournisseur de contenus, dans un délai de 48 heures à compter de la réception des informations concernant les motifs du retrait et les possibilités de recours.

En cas de constat de violation, l'autorité compétente adopte une décision motivée après en avoir informé l'autorité compétente ayant émis l'injonction de retrait. Elle communique ensuite sa décision à l'autorité compétente qui a émis l'injonction de retrait, au fournisseur de services d'hébergement, au fournisseur de contenus ayant demandé l'examen approfondi et, conformément à l'article 14, à Europol.

Cette décision de motivation produit deux conséquences principales :

- l'injonction de retrait cesse de produire des effets juridiques ;
- le fournisseur de services rétablit immédiatement le contenu ou l'accès à celui-ci.

b. Recours du fournisseur de services (article 9)

Le fournisseur de services peut contester l'injonction de retrait devant les juridictions de l'État membre de l'autorité compétente qui a émis l'injonction, mais également toute une série d'autres décisions visées aux articles 4, § 4, 5, § 4, 6 ou 7.

c. Recours du fournisseur de contenus (articles 9 et 10)

En cas de retrait de contenus terroristes ou de blocage de l'accès à ces contenus, leur fournisseur dispose d'un droit de recours effectif. En effet, il a le droit de contester l'injonction de retrait devant les juridictions de l'État membre de l'autorité compétente qui a émis l'injonction ainsi que de contester la décision d'une non-violation du règlement ou des droits et libertés consacrés par la Charte devant les juridictions de l'État membre de l'autorité compétente qui a rendu cette décision.

De plus, le fournisseur de contenus peut introduire une réclamation auprès du fournisseur de services s'il estime que le retrait de ses contenus ou le blocage de l'accès à ses contenus opéré en vertu de l'article 5 était injustifié.

2. Sanctions (article 18)

Le non-respect de plusieurs obligations prévues par le règlement est passible de sanctions, dont la détermination et la mise en œuvre relèvent de la compétence des États :

- obligation de retrait par le fournisseur de services (article 3, § 3 et article 4, § 2) ;
- obligation de l'information de retrait (article 3, § 6) ;

[44] Ligue des droits humains, « Le règlement européen sur les contenus à caractère terroriste en ligne et les droits fondamentaux », 1er février 2021, https://www.liguedh.be/le-reglement-europeen-sur-les-contenus-a-caractere-terroriste-en-ligne-et-les-droits-fondamentaux/.

- obligation de restauration des contenus en cas de décision constatant une violation du règlement ou des libertés et droits fondamentaux garantis par la Charte (article 4, § 7) ;
- obligation de mise en place de mesures spécifiques par le fournisseur de services (article 5, §§ 1 à 3 et §§ 5 à 6) ;
- obligation de conservation des contenus et des données connexes (article 6) ;
- obligation de transparence des fournisseurs de services d'hébergement (article 7) ;
- obligation pour les fournisseurs de services d'établir un mécanisme de réclamation à destination des fournisseurs de contenus (article 10) ;
- obligation d'information des fournisseurs de contenus par les fournisseurs de services en cas de retrait ou blocage (article 11) ;
- obligation d'information par les fournisseurs de services des autorités compétentes pour les enquêtes et les poursuites en matière d'infractions pénales lorsqu'ils prennent connaissance d'un contenu à caractère terroriste présentant une menace imminente pour la vie (article 14, § 5) ;
- obligation pour les fournisseurs de services d'établir un point de contact pour la réception et le traitement des injonctions (article 15, § 1er) ;
- obligation de désignation d'un représentant légal pour les fournisseurs de services d'hébergement dont l'établissement principal n'est pas situé dans l'Union (article 17).

Précisons également qu'en cas de violation persistante de l'obligation de retrait des contenus à la suite d'une injonction visée à l'article 3, § 3, les États membres sont tenus de prévoir des sanctions financières pouvant atteindre jusqu'à 4 % du chiffre d'affaires mondial du fournisseur de services d'hébergement pour l'exercice précédent.

II. LES MISES EN ŒUVRE NATIONALES : LES EXEMPLES FRANÇAIS ET BELGE

Pour rappel, le règlement vise à déterminer les mesures à prendre par les États pour identifier les contenus terroristes, veiller à leur retrait et faciliter la collaboration entre les différents acteurs impliqués. Quelles sont les procédures mises en place par les États ? Revenons dans un premier temps sur la loi Avia et sa censure par le Conseil constitutionnel français (A), pour détailler ensuite la situation actuelle en Belgique (B).

A. La loi Avia et le Conseil constitutionnel français

La France a adopté, le 24 juin 2020, la loi Avia, visant à lutter contre les contenus haineux sur Internet[45], dont les contenus terroristes. Quel dispositif la France a-t-elle mis en place ? S'inscrit-il dans la même lignée que le règlement (UE) 2021/784 ?

La loi Avia s'inscrit dans un contexte d'exacerbation des discours de haine dans la société, particulièrement sur Internet. Or, les dispositions applicables résultaient principalement de la loi du 21 juin 2004 pour la confiance dans l'économie numérique[46], « alors que les réseaux sociaux que nous connaissons aujourd'hui n'étaient pas encore accessibles en France ». Face à un constat d'impunité de la cyber-haine, le législateur français s'est donc attelé à la mise en place de « dispositions fortes et efficaces » afin de poursuivre l'objectif d'intérêt général que constitue la lutte contre les contenus haineux sur Internet[47].

[45] Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet (1), *J.O.R.F.*, n° 0156, 25 juin 2020.

[46] Loi du 21 juin 2004 pour la confiance dans l'économie numérique, *J.O.R.F.*, n° 0143, 22 juin 2004.

[47] Proposition de loi visant à lutter contre la haine sur internet n° 1785 du 20 mars 2019, https://www.

Néanmoins, le Conseil constitutionnel[48] a censuré la majeure partie des dispositions de cette loi, qu'elle a considérées comme contraires à la Constitution pour trois raisons principales.

Tout d'abord, le Conseil constitutionnel estime que « le législateur a porté à la liberté d'expression et de communication une atteinte qui n'est pas adaptée, nécessaire et proportionnée au but poursuivi »[49] en raison de la compétence de reconnaissance du caractère illicite d'un contenu. En effet, l'appréciation dépend de la seule administration, sans intervention du juge.

Ensuite, le délai limité pour le retrait, assorti d'une peine en cas de non-respect, pourrait amener les éditeurs ou hébergeurs à retirer tous les contenus signalés, même ceux ne présentant pas un caractère illicite, afin d'échapper à la sanction pénale[50].

Enfin, le Conseil constitutionnel souligne que « de nombreuses qualifications pénales justifi[e]nt le retrait de ces contenus ». Or, les éléments constitutifs de certaines de ces infractions peuvent « présenter une technicité juridique »[51], notamment dans le cas des infractions terroristes, qui ne relèvent pas des compétences des éditeurs et hébergeurs[52]. De plus, cette difficulté d'interprétation est exacerbée par le très court délai de réaction pour qualifier les contenus[53]. La Cour constitutionnelle belge a rendu un arrêt le 14 mars 2019[54], reprenant le même argument. En effet, elle a annulé l'obligation de dénonciation active imposée aux travailleurs sociaux prévue à l'article 46*bis*/1, § 3, du Code d'instruction criminelle. En vertu de celle-ci, les travailleurs sociaux étaient tenus de divulguer les informations, même couvertes par le secret professionnel, pouvant constituer des indices sérieux d'une infraction terroriste visée au Livre II, Titre I^er^*ter*, du Code pénal. La Cour a estimé que les infractions terroristes sont des infractions complexes qui requièrent la réunion de plusieurs éléments constitutifs. Or, elle a considéré que les travailleurs sociaux n'avaient « ni la compétence, ni les moyens nécessaires » pour évaluer si le comportement d'un allocataire ou d'un assuré social était constitutif d'une infraction terroriste visée au Livre II, Titre I^er^*ter*, du Code pénal[55].

Par conséquent, la loi Avia a été en grande partie annulée[56]. Nous reviendrons plus en détail dans notre troisième partie sur les arguments soulevés par la Cour, notamment en matière de principe de légalité et de liberté d'expression.

B. La situation belge

Bien que le règlement soit « obligatoire dans tous ses éléments et […] directement applicable dans tout État membre »[57], la Belgique

assemblee-nationale.fr/dyn/15/textes/l15b1785_proposition-loi#, Exposé des motifs.

48 Conseil constitutionnel français, décision n° 2020-801 DC du 18 juin 2020, *J.O.R.F.*, n° 0156, 25 juin 2020.

49 Conseil constitutionnel français, décision n° 2020-801 DC du 18 juin 2020 précitée, § 6.

50 Conseil constitutionnel français, décision n° 2020-801 DC du 18 juin 2020 précitée, §§ 6 et 13.

51 Conseil constitutionnel français, décision n° 2020-801 DC du 18 juin 2020 précitée, § 14.

52 Nous précisons.

53 Conseil constitutionnel français, décision n° 2020-801 DC du 18 juin 2020 précitée, § 15.

54 C. const., arrêt n° 44/2019 du 14 mars 2019.

55 E. Delhaise, « La dénonciation en matière de terrorisme : coup d'arrêt de la Cour constitutionnelle », www.justice-en-ligne.

56 En effet, les paragraphes I et II de l'article 1^er^ ; les articles 3, 4, 5, 7, 8, 9 ; les mots « et à l'avant-dernier alinéa du I de l'article 6-2 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, » figurant au second alinéa de l'article 10 ; le 1° de l'article 12 ; les mots « 4 et 5 ainsi que les I, II et III de l'article 7 » figurant à la première phrase de l'article 18 et la seconde phrase de ce même article ; le paragraphe II de l'article 19 et les articles 11 et 12, 2° et 3° ont été jugés contraires à la Constitution française.

57 T.F.U.E., art. 288.

devra répondre de ses obligations européennes d'ici le mois de juin 2022 en désignant, notamment, l'autorité compétente pour l'émission des injonctions de retrait.

Le présent point analysera dans un premier temps le régime applicable pour un autre type de criminalité, à savoir la pédopornographie (1) pour étudier dans un second temps les dispositifs existants en matière de terrorisme ainsi que les perspectives de mise en œuvre du règlement (2).

1. *Un précédent belge : la lutte contre la pédopornographie sur Internet*

Le retrait des contenus terroristes s'inscrit, comme nous l'avons remarqué précédemment, dans un contexte plus global de lutte contre la diffusion de contenus illicites sur Internet. Dans ce sens, nous avons précédemment évoqué la directive 2011/93/UE du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie[58]. Celle-ci définit les contenus pédopornographiques[59], incrimine plusieurs comportements en matière d'abus et violences sexuels et établit les mesures à prendre par les États contre les sites internet contenant ou diffusant de la pédopornographie[60]. Comment la Belgique s'est-elle, il y a dix ans, conformée à ses obligations européennes en la matière ? Revenons brièvement sur les mécanismes applicables pour retirer du contenu illicite diffusé en ligne dans le domaine de la pédopornographie (b), après avoir exposé les infractions prévues par le Code pénal belge (a).

a. Les infractions

La pédopornographie est incriminée à l'article 383*bis* du Code pénal belge et est sanctionnée d'une peine de réclusion de cinq ans à dix ans et d'une amende de cinq cents euros à dix mille euros (diffusion du contenu) ou d'une peine d'emprisonnement d'un mois à un an et d'une amende de cent euros à mille euros (possession du contenu).

Le contenu illicite est dans ce cas le matériel pédopornographique, défini dans ce même article 383*bis*, § 4, à savoir :

« 1° tout matériel représentant de manière visuelle, par quelque moyen que ce soit, un mineur se livrant à un comportement sexuellement explicite, réel ou simulé, ou représentant les organes sexuels d'un mineur à des fins principalement sexuelles ;

2° tout matériel représentant de manière visuelle, par quelque moyen que ce soit, une personne qui paraît être un mineur se livrant à

58 Directive 2011/93/UE précitée, L 335/1.

59 « i) tout matériel représentant de manière visuelle un enfant se livrant à un comportement sexuellement explicite, réel ou simulé ; ii) toute représentation des organes sexuels d'un enfant à des fins principalement sexuelles ; iii) tout matériel représentant de manière visuelle une personne qui paraît être un enfant se livrant à un comportement sexuellement explicite, réel ou simulé, ou toute représentation des organes sexuels d'une personne qui paraît être un enfant, à des fins principalement sexuelles ; ou iv) des images réalistes d'un enfant se livrant à un comportement sexuellement explicite ou des images réalistes des organes sexuels d'un enfant à des fins principalement sexuelles », directive 2011/93/UE précitée, art. 2, c).

60 « 1. Les États membres prennent les mesures nécessaires pour faire rapidement supprimer les pages internet contenant ou diffusant de la pédopornographie qui sont hébergées sur leur territoire et s'efforcent d'obtenir la suppression des pages hébergées en dehors de celui-ci.
2. Les États membres peuvent prendre des mesures pour bloquer l'accès par les internautes sur leur territoire aux pages internet contenant ou diffusant de la pédopornographie. Ces mesures doivent être établies par le biais de procédures transparentes et fournir des garanties suffisantes, en particulier pour veiller à ce que les restrictions soient limitées à ce qui est nécessaire et proportionnées, et que les utilisateurs soient informés de la raison de ces restrictions. Ces garanties incluent aussi la possibilité d'un recours judiciaire », directive 2011/93/UE précitée, art. 25.

un comportement sexuellement explicite, réel ou simulé, ou représentant les organes sexuels de cette personne, à des fins principalement sexuelles ;

3° des images réalistes représentant un mineur qui n'existe pas, se livrant à un comportement sexuellement explicite, ou représentant les organes sexuels de ce mineur à des fins principalement sexuelles ».

Précisons que cette liste n'est pas limitative et que toutes les formes de mise en réseau informatique sont visées[61], d'où l'expression « par quelque moyen que ce soit ». Cela permet ainsi d'anticiper l'éventuelle apparition de nouveaux types de supports[62].

b. Le retrait du contenu

L'Union européenne, par le biais de sa directive, entendait non seulement réprimer la diffusion de contenus pédopornographiques, mais également assurer le retrait et la suppression de tels contenus. Quels sont les mécanismes applicables en Belgique pour retirer ces contenus illicites diffusés en ligne ?

La question du retrait du contenu pédopornographique doit s'analyser en deux étapes : le signalement du contenu et la suppression du contenu.

L'article 383*bis*/1 du Code pénal prévoit qu'une organisation agréée par le Roi peut de droit recevoir des signalements relatifs aux contenus pédopornographiques. L'organisation désignée en Belgique est Child Focus, en vertu de l'arrêté royal portant agrément de Child Focus en tant qu'organisation visée à l'article 383*bis*/1 du Code pénal[63]. Child Focus est dès lors chargée de transmettre les signalements de sites internet hébergés sur des serveurs en Belgique aux services de police et aux autorités judiciaires belges ainsi que de transmettre à l'INHOPE[64], pour suite voulue, les signalements de pédopornographie en ligne hébergée sur des serveurs à l'étranger et d'en informer les services de police et les autorités judiciaires belges[65].

À la suite d'un « signalement Child Focus », quel sort est réservé aux contenus pédopornographiques par la loi belge ? Child Focus n'intervient pas dans l'appréciation de l'opportunité de rechercher et de poursuivre des infractions[66], l'organisation étant agréée pour les signalements uniquement. Ce sont donc les destinataires du signalement qui sont chargés de la suite à donner aux contenus pédopornographiques. Ces destinataires sont les services de police et les autorités judiciaires. Par conséquent, le retrait de contenus pédopornographiques relève du champ pénal et de la procédure pénale.

Le droit de la procédure pénale belge ne connait pas la figure du blocage de sites internet en tant que telle. Seul l'article 39*bis* du Code d'instruction criminelle permet au procureur du Roi ou au juge d'instruction d'ordonner la saisie de données informatiques[67].

61 N. Colette-Basecqz, « La protection pénale des personnes vulnérables dans l'environnement numérique », in M. Nihoul et H. Jacquemin (dir.), *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, p. 172.

62 N. Colette-Basecqz, « Pédopornographie et technologies : les réponses du droit pénal », in E. Degrave *et al.*, *Law, Norms and Freedoms in Cyberspace / Droits, normes et libertés dans le cybermonde. Liber Amicorum Yves Poullet*, Bruxelles, Larcier, 2018, p. 85.

63 Arrêté royal portant agrément de Child Focus en tant qu'organisation visée à l'article 383*bis*/1 du Code pénal, *M.B.*, 18 novembre 2016, p. 77087.

64 Internet Hotlines for Europe.

65 G. Mathieu et A.-C. Rasson, « Les droits de l'enfant dans l'environnement numérique : à la recherche d'un subtil équilibre entre protection et autonomie », in M. Nihoul et H. Jacquemin (dir.), *Vulnérabilités et droits dans l'environnement numérique*, *op. cit.*, p. 455.

66 *Ibid.*, p. 455.

67 C. Forget, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict ? », *R.D.T.I.*, 2017, p. 39.

En effet, en vertu de l'article 39*bis*, « les règles de ce code relatives à la saisie, y compris l'article 28*sexies*, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique ou une partie de celui-ci ». Cette saisie couvre donc à la fois la copie, le blocage et le retrait de données[68].

Néanmoins, cette solution ne nous convainc pas dans le cadre de la question du retrait des contenus illicites en raison du caractère provisoire de la saisie. En effet, la saisie est « une mesure conservatoire, prise dans le cadre de l'information, de l'instruction, de l'enquête particulière sur les avantages patrimoniaux ou de l'enquête pénale d'exécution par laquelle l'autorité compétente soustrait une chose au droit de libre disposition de son propriétaire ou de son possesseur et se saisit de cette chose en vue de la manifestation de la vérité, de la confiscation, de la restitution ou de la sécurité des intérêts civils »[69]. Le retrait est donc temporaire, ce qui ne semble pas rencontrer les objectifs de lutte contre la pédopornographie.

Une fois saisis, les contenus pédopornographiques peuvent faire l'objet d'une confiscation spéciale visée à l'article 42 du Code pénal. En effet, cette peine accessoire s'applique aux choses formant l'objet de l'infraction de pédopornographie de l'article 383*bis* du Code pénal, à savoir « les emblèmes, les objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pédopornographique »[70]. Précisons évidemment que le matériel informatique ayant servi à la commission de l'infraction peut également être confisqué en vertu de l'article 42, 1°, du Code pénal.

Nous pouvons donc constater que la procédure mise en place en matière de lutte contre la pédopornographie est une procédure judiciaire. Concernant le retrait des contenus, ceux-ci peuvent être provisoirement écartés puis définitivement retirés via les mécanismes successifs de la saisie puis de la confiscation. Qu'en est-il des contenus terroristes ? Un tel système pourrait-il trouver à s'appliquer ?

2. La lutte contre le terrorisme

Le point 1 nous a permis de fournir un aperçu des mécanismes existants en matière de lutte contre les contenus illicites, en illustrant nos propos via la problématique de la pédopornographie. Qu'en est-il de la lutte contre le terrorisme sur Internet, en Belgique ? Revenons, comme en matière de pédopornographie, sur les infractions terroristes commises sur Internet (a, b et c) pour nous intéresser ensuite à la possibilité de retrait des contenus terroristes (d).

a. Les infractions terroristes commises sur Internet : l'incitation, le recrutement et la formation

Les infractions terroristes sont visées au Livre II, Titre I^er^*ter*, du Code pénal belge. Trois infractions peuvent être commises sur Internet : l'incitation, le recrutement et la formation.

Tout d'abord, l'article 140*bis* du Code pénal incrimine la diffusion ou la mise à disposition intentionnelle du public d'un message créant le risque qu'une ou plusieurs infractions terro-

68 P. Monville, M. Giacometti et L. Grisard, « La collecte de preuves numériques en droit belge après l'arrêt de la Cour constitutionnelle du 5 décembre 2018 », https://orbi.uliege.be.

69 F. Lugentz et D. Vandermeersch, *Saisie et confiscation en matière pénale*, coll. Répertoire pratique du droit belge, Bruxelles, Larcier, 2015, p. 99 et Cass., 25 février 2003, R.G. P.02.0674.N, *Pas.*, 2003, n° 133.

70 F. Kuty, *Principes généraux du droit belge*, t. IV : *La peine*, Bruxelles, Larcier, 2017, p. 307.

ristes (infraction terroriste au sens strict ou voyage à visée terroriste) soient commises. Tous les modes de diffusion sont concernés : les forums internet, les réseaux sociaux, les sms multidestinataires, les meetings publics, les prêches, les conférences, la presse écrite ou parlée[71]. Ce qui importe, dans le cadre de l'incitation à commettre une infraction terroriste, est que le message diffusé ou mis à disposition du public crée un risque qu'une ou plusieurs infractions terroristes soient commises[72]. La création d'un tel risque a été considérée par le législateur comme une garantie contre la répression d'actes sans rapport avec le terrorisme[73].

Ensuite, le recrutement pour commettre une infraction terroriste au sens strict, pour participer aux activités d'un groupe terroriste ou diriger un tel groupe ou pour voyager à des fins terroristes est incriminé à l'article 140*ter* du Code pénal. Ce recrutement n'est pas défini, il convient donc de lui donner son sens courant, à savoir « le fait d'enrôler des recrues ou d'amener quelqu'un à entrer dans un groupe »[74]. Le recruteur approche une personne pour qu'elle commette une infraction terroriste au sens strict, qu'elle rejoigne les rangs d'un groupe terroriste ou qu'elle voyage à des fins terroristes[75]. Le « candidat terroriste » peut être approché de diverses manières, notamment sur Internet.

Enfin, l'infraction de formation en matière de terrorisme est incriminée aux articles 140*quater* et *quinquies* du Code pénal. La formation peut être définie comme « des instructions pour des méthodes et techniques propres à être utilisées à des fins terroristes, y compris pour la fabrication d'armes ou substances nocives ou dangereuses mais également d'autres méthodes ou techniques, telles que, par exemple, des cours de conduite ou de pilotage ou de hacking de site internet »[76]. Ces instructions peuvent être divulguées ou consultées via Internet. Trois comportements liés à cette formation sont constitutifs d'une infraction visée aux articles 140*quater* et suivants :

- le fait de dispenser la formation : fourniture intentionnelle de « connaissances terroristes » par un formateur à un élève ;
- le fait de recevoir la formation : acquisition intentionnelle de « connaissances terroristes » par un élève, par l'intermédiaire d'un formateur ;
- le fait de s'auto-former : formation de l'auteur via une démarche active et consciente[77]. Il ne s'agit plus dans ce cas d'obtenir des connaissances par l'intermédiaire d'un formateur mais bien de se former de manière proactive[78].

71 A. Masset, « Terrorisme », *Postal Memorialis – Lexique du droit pénal et des lois particulières*, Kluwer, février 2018, T 90/17.

72 E. Delhaise, *Infractions terroristes*, coll. Répertoire pratique du droit belge, Bruxelles, Larcier, 2019, p. 51.

73 Projet de loi du 13 novembre 2012 modifiant le Titre I^er^*ter* du Code pénal, *Doc. parl.*, Ch. repr., sess. ord. 2012-2013, n° 53/2502-001, Exposé des motifs, p. 12 ; C. const., arrêt du 15 mars 2018, n° 31/2018, www.cour-const.be, B.7.3. et A. Fransen et J. Kerkhofs, « Het materieel terrorismestrafrecht in België : de misdrijven », *T. Straf.*, 2018, p. 170.

74 *Le petit Larousse 2019*.

75 E. Delhaise, *Infractions terroristes*, *op. cit.*, p. 55.

76 I. de la Serna, « Des infractions terroristes », in Chr. De Valkeneer et I. de la Serna (coord.), *À la découverte de la justice pénale : paroles de juriste*, Bruxelles, Larcier, 2015, p. 224 et A. Fransen et J. Kerkhofs, « Het materieel terrorismestrafrecht in België : de misdrijven », *op. cit.*, p. 176.

77 Proposition de loi du 6 février 2019 portant des dispositions diverses en matière pénale et en matière de cultes, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54/3515-001, Exposé des motifs, p. 106 et M.-L. Cesoni, « Les infractions terroristes », in Chr. De Valkeneer et H.-D. Bosly (dir.), *Actualités en droit pénal 2019*, Bruxelles, Larcier, 2019, p. 238.

78 E. Delhaise, *Infractions terroristes*, *op. cit.*, p. 61.

b. Vers une incrimination de l'apologie du terrorisme ?

La Belgique a intégré les infractions terroristes dans son arsenal pénal en 2003 et complète celui-ci depuis 2013. La dernière proposition de loi vise à incriminer l'apologie du terrorisme[79]. Précisons néanmoins que cette infraction avait déjà fait l'objet de deux propositions de loi en 2015[80].

Le racisme, l'incitation aux discriminations ou encore le négationnisme font déjà l'objet d'incriminations pénales[81]. Cependant, la nécessité de lutter contre le terrorisme et le développement du phénomène de radicalisation amènent le législateur à sanctionner pénalement un nouveau comportement à l'article 140*octies* du Code pénal[82]. L'apologie du terrorisme s'entend comme le fait de « nie[r], minimise[r] grossièrement, cherche[r] à justifier ou approuve[r] la commission d'une ou de plusieurs infractions visées Titre I^er^*ter* ». Le législateur distingue l'apologie du terrorisme dans les conditions de publicité de l'article 444 du Code pénal (calomnie et diffamation)[83] et l'apologie du terrorisme par le biais des technologies de l'information et de la communication.

Concernant l'apologie du terrorisme via les technologies de l'information et de la communication, le législateur constate qu'« Internet constitue à cet égard un formidable outil pour les radicaux de tous bords (qu'ils soient d'ailleurs islamistes ou pas) ; ce réseau fourmille notamment de sites qui constituent une véritable "djihadosphère" »[84]. Par conséquent, une circonstance aggravante est prévue lorsque l'apologie est « virtuelle » en raison du fait que le mode de diffusion a une portée plus large, justifiant la différence de traitement et la peine plus sévère que pour l'apologie « réelle ». La peine sera aggravée plus lourdement encore lorsque le discours est relayé sur des sites fréquentés par des mineurs (les réseaux sociaux, par exemple)[85].

c. Contenus terroristes au sens du règlement ?

Les contenus diffusés par les auteurs des infractions d'incitation, de recrutement, de formation et d'apologie peuvent-ils être considérés comme des « contenus terroristes » au sens du règlement 2021/784 ?

Pour rappel, la diffusion de contenus terroristes recouvre le fait de diffuser du « matériel qui incite à ou sollicite une personne pour commettre une infraction terroriste visée

[79] Proposition de loi du 11 mars 2021 modifiant le Code pénal, tendant à réprimer l'apologie du terrorisme en public et sur Internet, *Doc. parl.*, Ch. repr., sess. ord. 2020-2021, n° 55/1845-001.

[80] Proposition de loi du 18 novembre 2015 visant à réprimer l'apologie du terrorisme en public et sur Internet, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54/1467-001 et proposition de loi du 26 novembre 2015 punissant le fait de minimiser grossièrement, de chercher à justifier, d'approuver, ou de faire l'apologie d'une infraction terroriste ou de s'en réjouir, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54/1483-001.

[81] Proposition de loi du 11 mars 2021 modifiant le Code pénal, tendant à réprimer l'apologie du terrorisme en public et sur Internet précitée, Exposé des motifs, p. 19.

[82] Proposition de loi du 11 mars 2021 modifiant le Code pénal, tendant à réprimer l'apologie du terrorisme en public et sur Internet précitée, Exposé des motifs, pp. 4-10.

[83] Propos tenus lors de réunions ou dans des lieux publics, dans des lieux non publics mais ouverts à un certain nombre de personnes ayant le droit de s'y rassembler, dans un lieu quelconque mais en présence d'une personne offensée et de témoins, écrits imprimés ou non, images ou emblèmes affichés, distribués ou vendus, mis en vente ou exposés au regard du public ou écrits non rendus publics mais adressés ou communiqués à plusieurs personnes.

[84] Proposition de loi du 11 mars 2021 modifiant le Code pénal, tendant à réprimer l'apologie du terrorisme en public et sur Internet précitée, Exposé des motifs, p. 8 et E. Paquette et A. Senecat, « Cyberguerre contre la djihadosphère », *L'Express*, 21 janvier 2015.

[85] Proposition de loi du 11 mars 2021 modifiant le Code pénal, tendant à réprimer l'apologie du terrorisme en public et sur Internet précitée, p. 22.

à l'article 3, §1er, points a) à i) de la Directive (UE) 2017/541, qui sollicite une (plusieurs) personne(s) pour participer aux activités d'un groupe terroriste, fournit des instructions concernant la fabrication ou l'utilisation d'explosifs, d'armes à feu ou d'autres armes, ou de substances nocives ou dangereuses, ou concernant d'autres méthodes ou techniques spécifiques afin de commettre ou contribuer à commettre une infraction terroriste ou qui constitue une menace quant à la commission d'une infraction terroriste »[86].

Concernant l'incitation, le recrutement et la formation, ces trois comportements sont explicitement visés par le règlement et sont même incriminés aux articles 5, 6 et 7 de la directive (UE) 2017/541. Par conséquent, un message diffusé sur Internet pour inciter à la commission d'une infraction, la prise de contact d'une personne via Internet pour qu'elle rejoigne un groupe terroriste ou la mise à disposition de connaissances terroristes sur Internet peuvent sans aucun doute être considérés comme des « contenus terroristes » au sens du règlement.

Concernant l'apologie du terrorisme, celle-ci n'est pas visée par le règlement. Rappelons qu'un règlement permet d'imposer la même obligation de manière uniforme dans l'ensemble de l'Union, est directement applicable, est gage de clarté et de sécurité juridique renforcée et évite les divergences de transposition dans les États membres. Le contenu faisant l'apologie du terrorisme ne peut donc pas être considéré comme du contenu terroriste au sens du règlement. Précisons cependant que le matériel diffusé afin de « promouvoir les activités d'un groupe terroriste » était considéré comme du contenu terroriste dans la proposition de règlement[87].

d. Le retrait des contenus terroristes

À l'instar des procédures de retrait des contenus pédopornographiques, nous devons analyser la question du retrait des contenus terroristes en deux temps : le signalement du contenu et la suppression de celui-ci.

Tout d'abord, avant de faire l'objet d'une injonction de retrait, l'existence du contenu terroriste doit être portée à la connaissance de l'autorité compétente. Deux questions se posent ici, face au silence du règlement concernant cette autorité compétente.

Premièrement, le Comité économique et social européen précise que l'injonction peut être émise « à titre de décision administrative ou judiciaire »[88]. Dans le cas de la lutte contre la pédopornographie, les saisies et confiscations sont ordonnées par les autorités judiciaires. Nous pouvons dès lors raisonnablement imaginer qu'un tel procédé pourrait également être appliqué en matière de lutte contre les contenus terroristes en ligne. Les autorités judiciaires feraient donc procéder à la saisie et à la confiscation des contenus terroristes qui leur auraient été signalés.

Deuxièmement, nous avons vu que les contenus pédopornographiques sont signalés par Child Focus aux services de police et aux autorités judiciaires, qui se chargent ensuite de la saisie et de la confiscation des données. La lutte contre le terrorisme étant actuellement une des priorités pour les services de renseignement et de police, ces deux services peuvent détecter des

86 Règlement (UE) 2021/784 précité, art. 2, 7).

87 Proposition COM(2018) 640 final de règlement précitée, art. 2, § 5, c).

88 Avis du Comité économique et social européen précité, § 3.6.

contenus terroristes[89]. En vertu de la loi organique des services de renseignement et de sécurité, « les services de renseignement et de sécurité, les services de police, les autorités administratives et judiciaires veillent à assurer entre eux une coopération mutuelle aussi efficace que possible »[90]. L'information peut donc parvenir aux autorités judiciaires via les services de renseignement ou de police. Précisons également que les fournisseurs de services d'hébergement procèdent au retrait de contenus, après les avoir détectés eux-mêmes. C'est notamment le cas de Facebook qui dispose d'un plan d'action « pour identifier, supprimer et empêcher la publication de contenus à caractère terroriste et la création de groupes, de pages ou de profils par des terroristes », notamment via l'intelligence artificielle et un algorithme[91]. Diverses sources d'informations existent dès lors déjà pour repérer les contenus terroristes. Néanmoins, nous pourrions envisager la création d'une structure spécifique, similaire à Child Focus ou à la CTIF[92].

Ensuite, les contenus terroristes diffusés sur Internet sont des données informatiques, au même titre que les contenus pédopornographiques. Par conséquent, ils peuvent faire l'objet de la mesure de saisie de données informatiques, que nous avons précédemment évoquée. Ainsi, les données peuvent être provisoirement retirées ou leur accès bloqué. Précisons également que dans le cadre d'une infraction de menace de commission d'un attentat terroriste (article 137, § 3, 6°, du Code pénal) ou d'incitation à la commission d'une infraction terroriste (article 140*bis* du Code pénal), en cas d'extrême urgence, le procureur du Roi ou le juge d'instruction peut ordonner verbalement que tous les moyens appropriés soient utilisés pour rendre inaccessibles les données qui forment l'objet de l'infraction ou ont été produites par l'infraction et qui sont contraires à l'ordre public ou aux bonnes mœurs[93]. À nouveau, ce retrait n'est que provisoire, ce qui ne répond pas aux objectifs de lutte contre la propagande terroriste en ligne.

À notre sens, les contenus terroristes pourraient faire l'objet d'une confiscation spéciale en tant que peine accessoire, au sens de l'article 42 du Code pénal. En effet, ceux-ci sont les choses sur lesquelles porte la matérialité des infractions[94] d'incitation, de recrutement, de formation ou de préparation. Dans le cadre de l'outrage public aux bonnes mœurs, les chansons, écrits, figures ou images contraires aux bonnes mœurs peuvent être confisqués[95]. Il nous semble dès lors que les textes, dessins, photos et manifestes présentant un caractère terroriste doivent pouvoir faire l'objet d'une telle peine accessoire. Si le fait de pouvoir confisquer des contenus terroristes nous semble autorisé et techniquement possible, au regard des pratiques mises en place pour lutter contre d'autres types de criminalité, deux questions doivent être posées pour permettre d'aller plus loin et de répondre aux besoins de la lutte contre le terrorisme.

89 H. Bosly, « Services de renseignement et justice pénale », in F. Kuty et A. Weyembergh (dir.), *La science pénale dans tous ses états*, Bruxelles, Larcier, 2019, p. 382.

90 Loi organique des services de renseignement et de sécurité du 30 novembre 1998, *M.B.*, 18 décembre 1998, p. 40312.

91 J. Braun et F. Laurent, « La lutte contre le terrorisme par la censure des "contenus à caractère terroriste": une ingérence justifiée au droit à la liberté d'expression ? », *R.B.D.I.*, 2018/2, p. 618.

92 Cellule de traitement des informations financières, « chargée d'analyser les faits et les transactions financières suspectes de blanchiment de capitaux ou de financement du terrorisme », https://finances.belgium.be/fr/sur_le_spf/institutions_qui_dependent_du_spf_finances/cellule_de_traitement_des_informations_financieres.

93 C.i.cr., art. 39*bis*, § 6, dernier alinéa.

94 F. Kuty, *Principes généraux du droit belge*, t. IV : *La peine*, *op. cit.*, p. 306.

95 *Ibid.*, p. 307.

Premièrement, quel sort réserver aux contenus terroristes confisqués ? En matière de stupéfiants ou d'armes, la loi prévoit la destruction des objets confisqués, supposés dangereux ou contraires à l'ordre public[96]. Au vu de la dangerosité des contenus terroristes et des potentielles conséquences dramatiques de leur diffusion massive, il nous semble qu'une telle possibilité pourrait être prévue par le Code pénal en matière de terrorisme.

Deuxièmement, la confiscation peut prendre la forme d'une peine accessoire, mais également d'une mesure de sûreté, « lorsqu'elle affecte des choses nuisibles ou dangereuses, qu'il faut retirer de la circulation »[97]. Cette dernière n'est pas une peine et ne dépend pas d'une condamnation pénale. L'autorité prononçant la confiscation-mesure de sûreté peut décider du sort à réserver à la chose confisquée et ordonner, notamment, sa destruction[98]. Précisons cependant que cette confiscation n'est autorisée que pour un nombre limité d'infractions, dont le terrorisme ne fait actuellement pas partie. Il serait donc nécessaire de modifier les dispositions applicables en matière de terrorisme pour pouvoir prononcer ce type de mesure.

III. LES CONTENUS TERRORISTES : DU TEXTE VAGUE DU RÈGLEMENT AUX INCIDENCES PRATIQUES ALARMANTES

Le règlement peut être critiqué pour diverses raisons (désignation de l'autorité compétente, délai de retrait des contenus, injonctions transfrontières…)[99]. Il nous semble cependant que le nœud des difficultés futures que pourrait poser la mise en œuvre de ce règlement est à trouver dans la définition centrale du règlement, à savoir les contenus terroristes. Les développements ultérieurs seront donc consacrés à la notion de contenus terroristes ainsi qu'à deux incidences pratiques alarmantes : l'identification automatisée (A) et le risque de censure non justifiée (B).

Les contenus terroristes sont définis de manière large et renvoient à des infractions terroristes définies de manière tout aussi large par la directive[100] (UE) 2017/541.

Tout d'abord, le contenu est défini comme « tout matériel », sans autre précision. Par conséquent, le matériel peut être visuel, sonore[101], écrit, parlé, dessiné… Cette définition large du matériel ne nous pose pas de question, elle permet justement d'englober tous les supports, y compris d'éventuels nouveaux supports qui feraient leur apparition dans les années à venir.

Ensuite, pour qualifier un contenu de terroriste, celui-ci doit inciter, solliciter ou préparer à la commission de l'infraction terroriste au sens strict. Or, toutes ces infractions pénales posent, à notre sens, question en termes de respect du principe de légalité. En effet, les différents éléments matériels requis (solliciter, inciter, former, préparer…) sont des comportements « on ne peut plus banals et anodins »[102]. De nombreux comportements pourraient donc se voir qualifiés de terroristes, du point de vue de l'élément matériel de ces infractions. Ce qui caractérise alors l'infraction terroriste est

96 F. Lugentz et D. Vandermeersch, *Saisie et confiscation en matière pénale*, *op. cit.*, p. 81.

97 F. Kuty, *Principes généraux du droit belge*, t. IV : *La peine*, *op. cit.*, p. 1185.

98 *Ibid.*, pp. 1187-1188.

99 Ligue des droits humains, « Le règlement européen sur les contenus à caractère terroriste en ligne et les droits fondamentaux », *op. cit.*

100 Directive (UE) 2017/541 précitée, art. 5, 6 et 7.

101 Contrairement aux contenus pédopornographiques, pour lesquels les matériels qui ne sont pas visuels sont exclus. N. Colette-Basecqz, « Pédopornographie et technologies : les réponses du droit pénal », *op. cit.*, p. 88.

102 Projet de loi du 22 juin 2015 visant à renforcer la lutte contre le terrorisme, *Doc. parl.*, Ch. repr., sess. ord. 2014-2015, n° 54/1198-001, Avis du Conseil d'État, p. 17 et M.-A. Beernaert, « Renforcement de l'arsenal législatif anti-terroriste : entre symboles et prévention », *J.T.*, 2015, p. 834.

l'intention de l'auteur[103]. Par conséquent, de nombreux contenus pourraient être considérés comme des contenus terroristes à tort, en raison de la définition vague de ces contenus et des infractions terroristes de manière plus générale. Le Comité économique et social européen avait d'ailleurs souligné l'importance de préciser « de manière aussi détaillée que possible les critères retenus pour définir certaines notions juridiques vagues »[104]. Le Comité n'a, selon nous, pas été entendu, les notions restant toujours floues.

Précisons enfin que la définition du contenu terroriste peut changer d'un État membre à l'autre[105]. En effet, le règlement renvoie à la directive qui prévoit des standards d'harmonisation des qualifications terroristes, sans imposer d'incriminations uniques. La notion de contenu terroriste peut donc varier selon l'État membre de localisation du fournisseur de services d'hébergement.

A. L'identification automatisée des contenus terroristes

Face à l'ampleur de la problématique de la propagande terroriste en ligne, le Conseil européen a souligné la nécessité de « [mettre] 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 »[106]. Il paraît effectivement évident de renforcer l'identification automatisée de tels contenus, les moyens humains semblant quantitativement impuissants face à la vague de contenus terroristes en ligne. Néanmoins, comme nous venons de le développer, la définition floue des contenus terroristes risque d'emporter des difficultés d'interprétation pour les mécanismes de détection automatisés, pour trois raisons principales.

Tout d'abord, le principe de légalité des incriminations est respecté, selon la Cour constitutionnelle belge et la Cour européenne des droits de l'homme, si le justiciable peut savoir « à partir du libellé de la disposition […] et au besoin à l'aide de son interprétation par les juridictions, quels actes et omissions engagent sa responsabilité pénale »[107]. Par conséquent, une marge d'interprétation laissée aux cours et tribunaux est tolérée dans le cadre du recours à des notions floues. Il nous semble évident que cette marge d'appréciation doit être humaine et judiciaire. En effet, rappelons les positions du Conseil constitutionnel français et de la Cour constitutionnelle belge concernant la qualification de comportements ou de contenus terroristes par des non juristes trop fastidieuse en raison de la complexité des éléments constitutifs. La marge d'appréciation laissée par la définition floue des contenus terroristes doit donc être entre les mains d'un juge et non d'un algorithme.

Ensuite, nous avons précédemment souligné que l'élément constitutif central en termes d'infractions terroristes est l'intention terroriste de l'auteur. Or, nous avons vu précédemment que le contenu diffusé « à des fins éducatives, journalistiques, artistiques ou de recherche, ou à des fins de prévention ou de lutte contre

103 Pour plus de détails concernant les infractions terroristes, voy. E. Delhaise, *Infractions terroristes*, *op. cit.*

104 Avis du Comité économique et social européen précité, § 4.4.

105 Avis du Comité économique et social européen précité, § 3.7.

106 Proposition COM(2018) 640 final de règlement précitée, p. 2.

107 Voy., parmi d'autres : Cour eur. D.H. (gde ch.), arrêt *Baskaya et Okçuoglu c. Turquie* du 8 juillet 1999, http://hudoc.echr.coe.int/eng?i=001-62828, § 39 ; Cour eur. D.H. (3e sect.), arrêt *E.K. c. Turquie* du 7 février 2002, http://hudoc.echr.coe.int/fre?i=001-64586, § 52 ; Cour eur. D.H. (gde ch.), arrêt *Kafkaris c. Chypre* du 12 février 2008, http://hudoc.echr.coe.int/eng?i=001-85018, § 141 ; Cour eur. D.H. (gde ch.), arrêt *Del Rio Prada c. Espagne* du 21 octobre 2013, http://hudoc.echr.coe.int/fre?i=001-127680, § 92 et C. const., arrêt n° 145/2012 du 6 décembre 2012, B.7.

le terrorisme, y compris le matériel qui représente l'expression d'opinions polémiques ou controversées dans le cadre du débat public, n'est pas considéré comme étant un contenu à caractère terroriste »[108]. C'est donc bien l'intention animant le fournisseur du contenu qui permettra de distinguer le contenu terroriste du contenu éducatif ou journalistique. Comment traduire cela en langage algorithmique ? La détection automatisée d'un contenu terroriste semble compromise, en raison du risque de confondre les messages visant à informer et à dénoncer le terrorisme et les véritables contenus terroristes[109].

Enfin, un troisième élément constitutif (outre les éléments matériel et moral) doit également être présent pour constituer une infraction terroriste, à savoir un élément contextuel. Or, « à la différence des humains, les algorithmes sont actuellement incapables d'évaluer le contexte culturel, de détecter l'ironie d'un discours ou de procéder à l'analyse critique requise pour reconnaître avec précision, par exemple, un contenu "extrémiste" ou un discours haineux »[110].

Par conséquent, malgré l'impossibilité humaine de faire face aux nombreux contenus terroristes diffusés en ligne, l'identification automatisée semble montrer ses limites. Il conviendrait dès lors d'opter pour une détection semi-automatisée, avec un premier filtre par intelligence artificielle, contrôlée ensuite par une démarche humaine. Cela permettrait, à notre sens, d'éviter d'engendrer une censure systématique de contenus pourtant non considérés comme terroristes et de préserver le droit à la liberté d'expression. Nous y revenons dans le point suivant.

B. Un risque exacerbé de censure non justifiée

La liberté d'expression est consacrée, notamment, par l'article 10 de la Convention européenne des droits de l'homme. L'objectif de cette contribution n'est pas de proposer une analyse du respect de la liberté d'expression en cas de retrait des contenus terroristes sur Internet[111]. Rappelons brièvement que le retrait ou le blocage de l'accès à des contenus constitue indéniablement une ingérence dans le droit à la liberté d'expression. Une ingérence dans cette liberté fondamentale est soumise au respect des exigences de l'article 10, § 2, à savoir qu'elle doit être prévue par la loi, être nécessaire dans une société démocratique et poursuivre un besoin social impérieux.

Nous souhaitons néanmoins alerter de deux risques de violation du principe de proportionnalité induits par le règlement.

Tout d'abord, nous avons constaté que les contenus terroristes étaient définis en des termes vagues. Ce manque de précision dans les contours de cette notion centrale est susceptible de mettre à mal la condition de proportionnalité requise par l'article 10, § 2, de la Convention européenne des droits de l'homme pour deux raisons principales.

108 Règlement (UE) 2021/784 précité, art. 1er, § 3.

109 J. Braun et F. Laurent, « La lutte contre le terrorisme par la censure des "contenus à caractère terroriste": une ingérence justifiée au droit à la liberté d'expression ? », *op. cit.*, p. 638.

110 Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye, A/73/348, 29 août 2018, § 29, cité par J. Braun et F. Laurent, « La lutte contre le terrorisme par la censure des "contenus à caractère terroriste": une ingérence justifiée au droit à la liberté d'expression ? », *op. cit.*, p. 634.

111 Nous renvoyons, sur la question du filtrage et du blocage de contenus, à la contribution suivante : Q. Van Enis, « Filtrage et blocage de contenus sur Internet au regard de la liberté d'expression », in C. de Terwangne et Q. Van Enis (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019, pp. 133-168.

Premièrement, parmi les autres obligations des fournisseurs de services d'hébergement, le règlement leur impose de mettre en œuvre des mesures préventives afin de détecter les contenus terroristes. Certains fournisseurs de services censurent eux-mêmes les contenus détectés. Or, comme nous l'avons remarqué dans la jurisprudence constitutionnelle française et belge, les qualifications terroristes présentent un certain degré de technicité et de complexité, requérant une interprétation. Des contenus pourraient donc être détectés à tort comme contenus terroristes, par des personnes non qualifiées pour ce genre d'appréciation, ce qui engendrerait une censure disproportionnée par rapport au but poursuivi et par conséquent, une violation du droit à la liberté d'expression.

Deuxièmement, les fournisseurs de services d'hébergement sont encouragés à avoir recours à des méthodes automatisées de détection des contenus terroristes. Nous avons néanmoins souligné les difficultés engendrées par l'identification par des algorithmes de tels contenus. Par conséquent, certains messages « risquent d'être assimilés aux véritables messages de propagande terroriste, et sont les cibles potentielles d'une censure *a priori* »[112], ne respectant dès lors pas la condition de proportionnalité requise par l'article 10, § 2.

Ensuite, le règlement prévoit des sanctions en cas de non-respect des injonctions de retrait, qui pourraient engendrer des « sur censures » ou des censures *a priori* pour se conformer aux obligations et échapper aux sanctions. Cela ne manque pas de nous alarmer en termes de respect du principe de proportionnalité exigé en cas d'ingérence dans le droit à la liberté d'expression.

CONCLUSION

Bien que le règlement poursuive le but légitime de lutter contre la propagande terroriste, besoin social impérieux au sens de l'article 10, § 2, de la Convention européenne des droits de l'homme, nous avons pu constater que plusieurs éléments doivent nous alerter, principalement concernant la notion de contenus terroristes.

En effet, ceux-ci, définis de manière insuffisamment précise, à notre sens, induisent plusieurs risques d'ingérence disproportionnée dans le droit à la liberté d'expression. La lutte contre le terrorisme est caractérisée par un difficile équilibre à trouver entre la protection de la vie des citoyens et le respect des droits humains. La lutte contre la propagande terroriste n'échappe pas à ce travail d'équilibriste. En effet, comme le souligne le Comité économique et social européen, il est nécessaire de lutter contre ce phénomène tout en luttant, dans le même temps, contre la censure ou l'autocensure sur Internet[113].

Concernant la Belgique, nous suivrons attentivement dans les prochains mois les suites données à ce règlement. Nous avons constaté qu'aucune procédure uniforme n'existait en Belgique, nous poussant à imaginer une procédure de retrait par application des principes généraux du droit de la procédure pénale belge. À l'inverse de la lutte contre la pédopornographie, il n'existe pas d'organisation centrale pour le signalement des contenus terroristes. Il serait certainement opportun de saisir l'occasion pour repenser le système belge et l'adapter à la fois aux impératifs de lutte contre le terrorisme et aux évolutions technologiques.

[112] J. Braun et F. Laurent, « La lutte contre le terrorisme par la censure des "contenus à caractère terroriste": une ingérence justifiée au droit à la liberté d'expression ? », *op. cit.*, p. 638.

[113] Avis du Comité économique et social européen précité, § 1.6.