

1.



Bruxelles, le 28.9.2017
COM(2017) 555 final

**COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU
CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ
DES RÉGIONS**

Lutter contre le contenu illicite en ligne

Pour une responsabilité accrue des plateformes en ligne

1. INTRODUCTION

Les plateformes en ligne sont des vecteurs importants d'innovation et de croissance dans l'économie numérique. Elles offrent des possibilités inouïes d'accès à l'information et d'échanges ainsi que de nouveaux débouchés commerciaux, en particulier aux petites et moyennes entreprises (PME). Les plateformes en ligne constituent aussi, aujourd'hui, le principal point d'accès à l'information et à divers contenus pour la plupart des gens, que ce soit par l'intermédiaire des moteurs de recherche, des réseaux sociaux, des sites de microblogage ou des plateformes de partage de vidéos. De plus, la récente évolution du modèle économique des plateformes se traduit par des liens plus étroits entre utilisateurs et contenu, notamment pour la publicité ciblée. Ces plateformes mettent en relation des milliards d'utilisateurs partageant de gros volumes de contenu et d'informations¹, et offrent des services innovants aux particuliers et aux entreprises.

Toutefois, la large diffusion de contenu illicite pouvant être mis, et donc consulté, en ligne suscite de sérieuses inquiétudes qui appellent une action résolue et efficace. **Ce qui est illicite hors ligne l'est aussi en ligne.** L'éloge du terrorisme, les discours xénophobes et racistes qui constituent des incitations publiques à la haine et à la violence ainsi que le matériel pédopornographique sont illicites dans l'UE. La présence croissante de matériel à caractère terroriste en ligne et la diffusion d'un tel contenu sont une menace sérieuse pour la sûreté et la sécurité ainsi qu'un affront à la dignité des victimes. L'Union européenne a répondu à ces préoccupations par un certain nombre de mesures², mais s'atteler à la détection et à la suppression du contenu illicite en ligne représente aujourd'hui un défi urgent pour la société numérique.

Préoccupé par une série d'attaques terroristes dans l'UE et la diffusion de propagande terroriste en ligne, le Conseil européen des 22 et 23 juin 2017 a déclaré qu'il: *«attend des entreprises du secteur qu'elles [...] mettent au point de nouvelles technologies et de nouveaux outils en vue d'améliorer la détection et la suppression automatiques des contenus qui incitent à la commission d'actes terroristes. Cela devrait être complété par les mesures législatives appropriées au niveau de l'UE, si nécessaire»*. Ces appels ont été réitérés dans les déclarations faites par les dirigeants des G7 et G20 à l'occasion de leurs récents sommets³. De même, le Parlement européen, dans sa résolution de juin 2017 sur les plateformes en ligne, a enjoint à celles-ci *«de renforcer leurs mesures de lutte contre les contenus en ligne illégaux et dangereux»* tout en invitant la Commission à présenter des propositions pour traiter ces problèmes⁴.

Les plateformes en ligne par lesquelles la plupart des internautes passent pour accéder au contenu ont la lourde responsabilité, vis-à-vis de la société, de protéger les utilisateurs, et plus généralement le public, et d'empêcher les criminels et autres personnes impliquées dans des activités délictueuses

¹ Aujourd'hui, à chaque seconde, environ 8 000 tweets sont postés sur Twitter, 1 000 photos sont postées sur Instagram, 60 000 recherches sont effectuées sur Google et 70 000 vidéos sont visionnées sur YouTube. Voir <http://www.internetlivestats.com/>

² Voir partie 2.

³ Conclusions du Conseil européen, ST 8 2017 INIT, 22 et 23 juin 2017, déclaration du G7 de Taormine, 26 mai 2017, et déclaration des dirigeants du G20, 8 juillet 2017.

⁴ Résolution du Parlement européen du 15 juin 2017 sur les plateformes en ligne [2016/2274(INI)].

d'exploiter leurs services. Les espaces numériques ouverts qu'elles créent ne doivent pas être le terreau, par exemple, de la terreur, des discours de haine, de la pédophilie ou de la traite des êtres humains, ni devenir des zones échappant à l'État de droit. Il est clair que la diffusion de contenu illicite en ligne peut entamer la confiance du public dans l'environnement numérique, mais elle pourrait aussi menacer le développement économique futur de l'écosystème des plateformes et du marché unique numérique. Du fait de la responsabilité découlant de leur rôle central dans la société, les plateformes numériques devraient résolument intensifier leurs actions pour traiter ce problème.

Il faut mener la lutte contre le contenu illicite en ligne avec des garanties solides et appropriées pour assurer la protection des divers droits fondamentaux en jeu. Étant donné la part de plus en plus importante qu'elles prennent dans la fourniture d'accès à l'information, les plateformes en ligne ont aussi un rôle clé à jouer pour établir cet équilibre. Dans la lutte contre le contenu illicite en ligne au sein de l'UE, il conviendrait de s'inspirer et de tenir compte des actions de l'UE au niveau mondial.

La présente communication prévoit un ensemble d'orientations et de principes afin que les plateformes en ligne intensifient la lutte contre le contenu illicite en ligne⁵ en coopération avec les autorités nationales, les États membres et les autres acteurs concernés. Elle vise à faciliter et à accélérer la mise en œuvre de bonnes pratiques pour interdire, détecter, supprimer et bloquer l'accès au contenu illicite de façon à garantir le retrait effectif de celui-ci, une transparence accrue et la protection des droits fondamentaux en ligne. Elle vise aussi à apporter aux plateformes des précisions sur leurs responsabilités lorsqu'elles prennent des mesures proactives (dites de «bon Samaritain») pour détecter, supprimer ou bloquer l'accès au contenu illicite.

2. CONTEXTE

L'Union européenne a déjà traité le problème du contenu illicite en ligne en prenant à la fois des mesures contraignantes et des mesures non contraignantes. Parmi ces réponses politiques figurent la directive relative à la lutte contre **les abus sexuels et l'exploitation sexuelle des enfants ainsi que la pédopornographie**⁶, la directive relative à la lutte contre **le terrorisme**⁷ et les mesures proposées dans le cadre des révisions du **droit d'auteur**⁸ et de la directive sur **les services de médias audiovisuels** (directive SMA)⁹.

⁵ Les éléments présentés ici reposent sur une série de consultations publiques et ciblées ainsi que d'ateliers réunissant les parties intéressées.

⁶ Voir le récent rapport de la Commission au Parlement européen et au Conseil sur l'évaluation de la mise en œuvre des mesures visées à l'article 25 de 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.

⁷ La directive (UE) 2017/541 relative à la lutte contre le terrorisme oblige les États membres à prendre les mesures nécessaires pour faire rapidement supprimer les contenus en ligne incitant à commettre des actes terroristes (article 21). Dans ce domaine, et dans le cadre du Forum de l'UE sur l'Internet, les plateformes suppriment volontairement les contenus à caractère terroriste sur la base des signalements transmis par l'unité de signalement des contenus sur Internet (IRU) d'Europol.

⁸ COM(2016) 593.

⁹ COM(2016) 287.

Ces mesures législatives, adoptées ou proposées, ont été complétées par une série de mesures non législatives comme le code de conduite visant à combattre les **discours de haine illégaux** en ligne¹⁰, les travaux du **Forum de l'UE sur l'Internet**¹¹ en ce qui concerne la **propagande terroriste**, le protocole d'accord sur la vente de **contrefaçons**¹², la communication de la Commission sur la **surveillance du marché pour les produits vendus en ligne**¹³, la vente en ligne de **produits de la chaîne alimentaire**, le plan d'action de l'UE contre le **trafic d'espèces sauvages**¹⁴, les orientations concernant la directive relative aux **pratiques commerciales déloyales**¹⁵ ou les actions communes des autorités nationales au sein du réseau de coopération en matière de protection des consommateurs¹⁶. La stratégie européenne pour un **Internet mieux adapté aux enfants**¹⁷ est une initiative d'autorégulation visant à améliorer l'environnement en ligne pour les enfants et les jeunes, étant donné les risques de confrontation, notamment, à du contenu violent ou des abus sexuels, ou de cyberintimidation.

Dans ses communications de 2016 et 2017¹⁸, la Commission a souligné la nécessité pour les plateformes en ligne d'avoir une attitude plus responsable et de faire davantage d'efforts d'autorégulation à l'échelle de l'UE pour supprimer le contenu illicite. En outre, la Commission s'est engagée à mieux coordonner les divers dialogues sectoriels avec les plateformes et à déterminer si des orientations concernant des procédures formelles de notification et d'action sont nécessaires. Cela doit se faire en tenant compte et sans préjudice des dialogues déjà engagés et des travaux entrepris dans d'autres domaines, notamment au titre du programme européen en matière de sécurité ou concernant les discours de haine illégaux.

Il ressort de récents rapports sur certaines de ces initiatives sectorielles que quelques progrès ont été accomplis. Pour ce qui est des discours de haine illégaux, des rapports de juin 2017 indiquaient une augmentation des contenus supprimés après signalement de 28 % à 59 % sur une période de six mois dans certains pays de l'UE, mais avec des différences importantes entre les plateformes¹⁹. Quelques progrès ont également été enregistrés sur la même période concernant la rapidité de suppression même si, dans encore 28 % des cas, ladite suppression n'intervient qu'au bout d'une semaine²⁰. Cela montre qu'une approche non réglementaire peut produire des résultats, en particulier lorsqu'elle s'accompagne de mesures visant à faciliter la coopération entre tous les acteurs concernés. Dans le cadre de la lutte du Forum de l'UE sur l'Internet contre les contenus à caractère terroriste, environ 80-90 % des contenus signalés par Europol ont été supprimés depuis le lancement du Forum²¹.

¹⁰ http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

¹¹ http://europa.eu/rapid/press-release_IP-15-6243_fr.htm

¹² <http://ec.europa.eu/transparency/regdoc/rep/3/2016/FR/3-2016-3724-FR-F1-1.PDF>

¹³ JO C 250 du 1.8.2017.

¹⁴ http://ec.europa.eu/environment/cites/pdf/WAP_EN_WEB.pdf

¹⁵ SWD(2016) 163 du 25.5.2016.

¹⁶ http://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/consumer_protection_cooperation_network/index_en.htm

¹⁷ COM(2012) 196 final, <https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online>

¹⁸ COM(2016) 288 et COM(2017) 228.

¹⁹ http://europa.eu/rapid/press-release_IP-17-1471_fr.htm

²⁰ http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=71674

²¹ http://europa.eu/rapid/press-release_IP-17-544_fr.htm.

Concernant le matériel pédopornographique, le réseau de lignes d'urgence INHOPE faisait déjà état, en 2015, d'un taux de suppression de 91 % dans les 72 heures, 1 contenu sur trois étant supprimé dans les 24 heures²².

Les divers dialogues sectoriels en cours ont aussi fait apparaître une grande similitude des procédures en matière de détection, d'identification, de suppression et d'interdiction de rechargement entre les différents secteurs. Ces conclusions ont étayé la présente communication.

Au niveau de l'UE, le cadre juridique général applicable à la suppression de contenu illicite est la directive sur le commerce électronique²³ qui, en particulier, harmonise les conditions dans lesquelles certaines plateformes en ligne peuvent bénéficier de la dérogation en matière de responsabilité concernant le contenu illicite qu'elles hébergent dans l'ensemble du marché unique numérique.

Sur les plateformes en ligne, le contenu illicite se répand surtout par l'intermédiaire des services qui permettent de mettre en ligne le contenu de tiers. Ces services d'hébergement sont, sous certaines conditions, couverts par l'article 14 de la directive sur le commerce électronique²⁴. Cet article dispose que les prestataires de services d'hébergement²⁵ ne peuvent être tenus responsables des informations stockées à la demande de tiers à condition qu'ils: a) n'aient pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'aient pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente; ou b) dès le moment où ils ont de telles connaissances, agissent promptement pour retirer les informations ou rendre l'accès à celles-ci impossible. En même temps, la directive doit «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**»²⁶.

De plus, l'article 15 interdit aux États membres d'«*imposer aux prestataires, pour la fourniture des services visée [à l'article 14], une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites*». En même temps, le considérant 47 de la directive rappelle que cette interdiction concerne uniquement les obligations de surveillance à caractère général et qu'«[e]lle ne concerne pas les obligations de surveillance applicables à un cas spécifique et,

²² http://www.inhope.org/Libraries/Annual_reports/INHOPE_Annual_Report_2015.sflb.ashx?download=true

²³ Directive 2000/31/CE du 8 juin 2000 sur le commerce électronique.

²⁴ Il faut signaler que, en vertu de la directive sur le commerce électronique, seuls bénéficient de la dérogation en matière de responsabilité visée aux articles 12-14 les prestataires de services de la société de l'information qui sont considérés comme des prestataires intermédiaires (c.-à-d. fournissant des services de simple transport, de stockage en antémémoire ou d'hébergement, selon le cas). Le considérant 42 précise que, pour que les activités donnent lieu à exemption de responsabilité, elles doivent revêtir «un caractère purement technique, automatique et passif, qui implique que le prestataire de services de la société de l'information n'a pas la connaissance ni le contrôle des informations transmises ou stockées».

²⁵ La plupart des plateformes en ligne offrent des services d'hébergement de contenu mis en ligne par leurs utilisateurs.

²⁶ Considérant 40 de la directive sur le commerce électronique. Il convient de signaler que la présente communication vise principalement les prestataires de services d'hébergement, plutôt que les fournisseurs de services de simple transport (article 12) ou de stockage en antémémoire (article 13).

notamment, elle ne fait pas obstacle aux décisions des autorités nationales prises conformément à la législation nationale».

À cet égard, dans sa communication de 2016, la Commission s'est engagée à maintenir un régime de responsabilité équilibré et prévisible pour les plateformes en ligne comme cadre réglementaire fondamental de l'innovation dans l'ensemble du marché unique numérique.

Les orientations contenues dans la présente communication sont sans préjudice de l'acquis de l'UE. Elles concernent les activités des plateformes en ligne, et en particulier les services d'hébergement fournis par ces plateformes²⁷ au sens de l'article 14 de la directive sur le commerce électronique, et couvrent toutes les catégories de contenu illicite mais tiennent dûment compte du fait que des types de contenu différents peuvent exiger des traitements différents.

Actuellement, il n'existe pas d'approche harmonisée et cohérente de la suppression du contenu illicite dans l'UE. De fait, plusieurs approches y coexistent, qui diffèrent en fonction des États membres, des catégories de contenu ou du type de plateforme en ligne. **Une approche plus homogène rendrait donc la lutte contre le contenu illicite plus efficace. Elle contribuerait aussi au développement du marché unique numérique** et à réduire le coût de mise en conformité avec une multitude de règles applicables aux plateformes en ligne, y compris pour les nouveaux entrants.

Il importe de souligner que ce cadre juridique ne vise pas à définir, et encore moins à harmoniser, ce qui constitue du contenu «illicite». **Ce qui est illicite est établi par la législation spécifique au niveau de l'UE ainsi que par les législations nationales**²⁸. Si, par exemple, le matériel à caractère terroriste, les discours de haine illégaux ou le matériel pédopornographique ou encore la traite des êtres humains sont, de par leur nature, leurs caractéristiques et le préjudice qu'ils causent, très différents des violations des droits de propriété intellectuelle ou des règles en matière de sécurité des produits, des pratiques commerciales illégales en ligne ou des activités en ligne à caractère diffamatoire, ces différents types de contenu illicite relèvent tous du même cadre juridique général instauré par la directive sur le commerce électronique. En outre, étant donné la grande similitude des *processus de suppression* de ces différents types de contenu, la présente communication couvre l'intégralité des contenus illicites en ligne, **des variations sectorielles étant admises dès lors qu'elles sont appropriées et justifiées.**

Dans l'UE, les tribunaux et les instances nationales compétentes, y compris les autorités chargées de faire respecter la loi, sont habilités à engager des poursuites criminelles et à infliger des sanctions

²⁷ Par «service d'hébergement» on entend un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service. Cela peut prendre diverses formes comme les places de marché en ligne, les plateformes de partage de vidéos, les réseaux sociaux, les sites Web de blogage ou d'avis ou les rubriques «commentaires» des pages d'actualités.

²⁸ Parmi les domaines soumis (ou qu'il est proposé de soumettre) au droit de l'UE, on peut citer l'éloge du terrorisme, les discours de haine illégaux, la pédopornographie, les droits de propriété intellectuelle, la sécurité des produits, l'offre et la vente de produits alimentaires ou du tabac et de médicaments de contrefaçon, les règles de protection des consommateurs ou les mesures en matière de sécurité des produits, etc. En 2016, la Commission a également précisé les obligations de transparence et de diligence professionnelle des plateformes en ligne, en vertu de la directive 2005/29/CE relative aux pratiques commerciales déloyales, lorsque les plateformes se comportent comme des professionnels vis-à-vis des consommateurs.

pénales, selon une procédure régulière, concernant l'illégalité d'une activité ou d'une information en ligne donnée. En même temps, les plateformes en ligne ont le droit d'empêcher que leur infrastructure et leur activité servent à commettre des crimes, ont la responsabilité de protéger leurs utilisateurs et d'interdire la présence de contenu illicite en leur sein et disposent généralement des moyens de repérer et de supprimer un tel contenu. Cela est d'autant plus important que les plateformes en ligne ont investi massivement pour mettre au point des techniques perfectionnées afin de recueillir, de façon proactive, des informations sur le contenu diffusé dans leurs structures et sur le comportement des utilisateurs. S'il est important de prendre des décisions rapides concernant la suppression du contenu illicite, il faut aussi appliquer des garanties suffisantes. Cela implique également une répartition équilibrée des rôles entre organismes publics et privés.

Les orientations et principes établis dans la présente communication n'ont donc pas comme seule finalité la détection et la suppression du contenu illicite. Ils visent aussi à dissiper les inquiétudes concernant la suppression du contenu *licite*, parfois désignée par «retrait abusif», laquelle a une incidence sur la liberté d'expression et le pluralisme des médias. Par conséquent, il faudrait prévoir des garanties suffisantes et adaptées au type spécifique de contenu illicite concerné.

S'il y a sans conteste des préoccupations d'intérêt général à propos du contenu qui n'est pas forcément illicite, mais potentiellement préjudiciable, comme les fausses informations ou le contenu préjudiciable aux mineurs²⁹, l'objectif de la présente communication est avant tout la détection et la suppression du **contenu illicite**.

3. DETECTER ET SIGNALER LE CONTENU ILICITE

Cette partie vise à **définir ce que les plateformes en ligne, les autorités compétentes et les utilisateurs devraient faire afin de détecter rapidement et efficacement le contenu illicite.**

Les plateformes en ligne peuvent apprendre l'existence de contenu illicite de plusieurs façons et par différents moyens de signalement, au nombre desquels: i) les décisions de justice ou administratives; ii) les notifications d'autorités compétentes (p. ex. celles chargées de faire respecter la loi), de «signaleurs de confiance», de titulaires de droits de propriété intellectuelle ou d'utilisateurs ordinaires; ou iii) les enquêtes ou découvertes qu'elles font elles-mêmes.

En plus de s'acquitter des obligations légales découlant du droit national et de l'UE, et de leur devoir de prudence dans le cadre de leurs responsabilités, les plateformes en ligne devraient garantir aux utilisateurs un environnement sûr, hostile à toute exploitation criminelle ou illégale et qui dissuade et empêche toute activité criminelle ou délictueuse en ligne.

²⁹ La proposition de révision de la directive sur les services de médias audiovisuels aborde ce sujet dans le contexte du contenu audiovisuel.

3.1. Tribunaux et autorités compétentes

Conformément au droit de l'UE et/ou national, les tribunaux nationaux et, dans certains cas, les autorités compétentes peuvent soumettre les plateformes en ligne à des injonctions ou des décisions administratives exigeant qu'elles suppriment ou bloquent l'accès au contenu illicite³⁰.

Comme la vitesse de suppression du contenu illicite est souvent déterminante pour enrayer sa diffusion et limiter le préjudice causé, les plateformes en ligne devraient pouvoir prendre des décisions rapides concernant les éventuelles mesures applicables au contenu illicite en ligne sans être mises en demeure de le faire par une injonction ou une décision administrative, surtout lorsqu'une autorité chargée de faire respecter la loi repère du contenu prétendument illicite et les en informe. En même temps, les plateformes en ligne, lorsqu'elles assument leurs responsabilités en la matière, devraient prévoir des garanties suffisantes afin de préserver le droit des utilisateurs à un recours effectif.

Les plateformes en ligne devraient donc disposer des ressources nécessaires pour bien comprendre les cadres juridiques dans lesquels elles opèrent. Elles devraient aussi **coopérer étroitement avec toute autorité chargée de faire respecter la loi ou compétente**, si nécessaire, notamment en veillant à ce qu'on puisse les contacter rapidement et efficacement en cas de demande de suppression immédiate de contenu illicite, ainsi que pour avertir l'autorité chargée de faire respecter la loi, si besoin est, de signes d'activité criminelle en ligne³¹. Pour éviter les doubles emplois et les notifications répétées et donc de nuire à l'efficacité et à l'efficacé du processus de suppression, les autorités chargées de faire respecter la loi ou compétentes devraient aussi s'efforcer de coopérer entre elles pour définir des interfaces numériques efficaces permettant la soumission rapide et fiable d'une notification, et garantir l'identification et le signalement efficaces du contenu illicite. Pour le bon déroulement de cette coopération, il est essentiel que les plateformes et les autorités établissent des points de contact.

Pour le contenu à caractère terroriste³², il a été créé au sein d'Europol une unité de signalement des contenus sur Internet (IRU) de l'UE, par l'intermédiaire de laquelle des experts de la sécurité évaluent et signalent tout contenu de cette nature aux plateformes en ligne (certains États membres disposent toutefois de leur propre IRU nationale).

³⁰ L'article 14, paragraphe 3, de la directive sur le commerce électronique précise que l'article 14 «n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette fin à une violation ou qu'il prévienne une violation». Par exemple, l'article 11 de la directive 2004/48/CE relative au respect des droits de propriété intellectuelle dispose que «[l]es États membres veillent également à ce que les titulaires de droits puissent demander une injonction à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit de propriété intellectuelle, sans préjudice de l'article 8, paragraphe 3, de la directive 2001/29/CE».

³¹ L'article 15, paragraphe 2, de la directive sur le commerce électronique dispose que «[l]es États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement».

³² Au sens de l'article 5 de la directive (UE) 2017/541 relative à la lutte contre le terrorisme.

Les plateformes en ligne devraient **systématiquement intensifier leur coopération avec les autorités compétentes des États membres, tandis que ceux-ci devraient veiller à ce que les tribunaux puissent effectivement sanctionner le contenu illicite en ligne** et à ce qu'il y ait une **coopération (transfrontière) plus étroite entre les autorités concernées.**

Les plateformes en ligne et les autorités chargées de faire respecter la loi ou compétentes devraient désigner des points de contact effectifs dans l'UE et, le cas échéant, définir des interfaces numériques efficaces pour faciliter leur interaction.

Les plateformes en ligne et les autorités chargées de faire respecter la loi sont également encouragées à mettre au point des **interfaces techniques qui leur permettent de coopérer plus efficacement du début à la fin du cycle de gestion du contenu.** La coopération avec la communauté technique peut aussi être utile pour progresser et apporter des solutions efficaces et techniquement viables à ce problème.

3.2. Notifications

3.2.1. Signaleurs de confiance

La suppression du contenu illicite en ligne est plus rapide et plus fiable lorsque les plateformes en ligne mettent en place des mécanismes qui fournissent aux notifiants ayant une expertise particulière un moyen privilégié de signaler la présence de contenu potentiellement illicite sur leur site Web. Il s'agit de ceux qu'on appelle «signaleurs de confiance», c'est-à-dire des entités spécialisées ayant des compétences précises en matière de repérage de contenu illicite, et des structures destinées à la détection et à l'identification d'un tel contenu en ligne.

Par rapport aux utilisateurs ordinaires, **les signaleurs de confiance sont censés apporter leur expertise et travailler selon des normes de qualité élevées** avec, pour résultat, des notifications de meilleure qualité et des retraits plus rapides. Les plateformes en ligne sont encouragées à recourir aux réseaux existants de signaleurs de confiance. Par exemple, pour le contenu à caractère terroriste, l'unité de signalement des contenus sur Internet d'Europol a l'expertise requise pour déterminer si un contenu donné constitue un contenu en ligne extrémiste à caractère terroriste et violent, et la met à profit pour jouer le rôle de signaleur de confiance, outre celui de faire respecter la loi. Le réseau de lignes d'urgence INHOPE pour le signalement de matériel pédopornographique constitue un autre exemple de signaleur de confiance. S'agissant des discours de haine illégaux, il existe des organisations de la société civile ou des organismes semi-publics qui sont spécialisés dans l'identification et le signalement des contenus racistes et xénophobes en ligne.

Afin de garantir la qualité des notifications et une suppression rapide du contenu illicite, **les entreprises pourraient convenir, au niveau de l'UE, de critères fondés notamment sur le respect des droits fondamentaux et des valeurs démocratiques.** Il est possible de définir les critères **en vertu desquels une entité particulière peut être considérée comme un signaleur de confiance** par le recours à des mécanismes d'autorégulation ou dans le cadre de la normalisation de l'UE, en prévoyant assez de souplesse pour prendre en compte les caractéristiques spécifiques au contenu et le rôle du signaleur de confiance. Sur la liste non exhaustive des autres critères pourraient figurer les normes internes de formation, les normes de processus et l'assurance de qualité ainsi que les

garanties juridiques concernant l'indépendance, les conflits d'intérêts et la protection de la vie privée et des données à caractère personnel. Ces garanties sont particulièrement importantes dans le petit nombre de cas où les plateformes peuvent supprimer du contenu après notification du signaleur de confiance sans vérifier elles-mêmes la légalité du contenu. Dans ces quelques cas, les signaleurs de confiance pourraient aussi être soumis à un contrôle selon les mêmes critères, et un système de certification pourrait attester leur statut. Dans tous les cas, il faudrait prévoir des garanties suffisantes pour prévenir une utilisation abusive du système, comme indiqué à la partie 4.3.

Les autorités compétentes devraient avoir la possibilité de prendre part, le cas échéant, aux mécanismes de signalement des signaleurs de confiance.

Un juste équilibre doit être trouvé entre la nécessité de garantir la qualité des notifications provenant des signaleurs de confiance, le champ d'application des mesures supplémentaires que les entreprises prendraient relativement à ces signaleurs et la charge qu'implique le respect de ces normes de qualité. Si les mécanismes d'un signaleur de confiance enfreignent les normes établies, le signaleur devrait se voir retirer son statut privilégié.

La Commission encourage une **étroite coopération entre les plateformes en ligne et les signaleurs de confiance. Les notifications des signaleurs de confiance devraient pouvoir être traitées de manière accélérée par la plateforme concernée.** Cette coopération devrait permettre un échange d'informations de sorte que le processus de suppression puisse être évalué et amélioré progressivement.

La Commission **étudiera** plus avant, notamment dans le cadre des dialogues avec les acteurs concernés, **les possibilités de convenir, à l'échelle de l'UE, de critères applicables aux signaleurs de confiance.**

3.2.2. *Notifications des utilisateurs*

Pour l'efficacité de la lutte contre le contenu illicite en ligne, les utilisateurs ordinaires devraient être habilités à signaler un tel contenu aux plateformes et avoir l'assurance que les notifications justifiées seront prises en considération et qu'il y sera donné suite rapidement.

Les plateformes en ligne devraient **instaurer un mécanisme aisément accessible et convivial qui permette à leurs utilisateurs de signaler** tout contenu, considéré comme illicite, qu'elles hébergeraient.

Si le contenu est accessible au public, ce mécanisme de signalement devrait être mis à la disposition du grand public, sans qu'il soit nécessaire de s'inscrire comme utilisateur. Pour que l'évaluation d'un contenu potentiellement illicite soit plus efficace et plus précise, un tel mécanisme devrait permettre une **notification facile par voie électronique.**

Dans sa proposition de révision de la directive sur les services de médias audiovisuels, la Commission entend imposer aux fournisseurs de plateforme de partage de vidéos l'obligation de mettre en place et d'utiliser des mécanismes permettant aux utilisateurs d'indiquer ou de signaler les contenus audiovisuels susceptibles de nuire à l'épanouissement physique, mental ou moral des mineurs, ainsi que les contenus comportant une incitation à la violence ou à la haine.

3.2.3. *Garantir la qualité des notifications*

Les plateformes en ligne devraient **mettre en place des mécanismes efficaces facilitant la soumission de notifications qui sont suffisamment précises et correctement étayées** pour leur permettre de prendre une décision rapide et en connaissance de cause sur la suite à y donner. Il serait ainsi plus facile de disposer de notifications qui contiennent une **explication des raisons** pour lesquelles le notifiant considère le contenu comme illicite et une indication claire de **l'emplacement** du contenu potentiellement illicite (p. ex. son adresse URL).

Ces mécanismes de signalement devraient être visibles, aisément accessibles, **conviviaux et contextuels**. Ils devraient aussi permettre de **signaler facilement** les différents types de contenu, p. ex. en choisissant dans une liste la catégorie de raisons pour lesquelles le contenu est considéré comme illicite. S'il est techniquement possible, le recours à des fonctions comme celles permettant de faire immédiatement une notification à la première occurrence du matériel, ou de réutiliser des identifiants d'inscription, est envisageable.

Lorsqu'elles sont suffisamment étayées et détaillées, ces notifications permettent à la plateforme de vite trouver le contenu potentiellement illicite, de faire une évaluation solide de l'illégalité du contenu et, le cas échéant, d'agir promptement. Le degré exact de détail requis par les plateformes pour pouvoir prendre rapidement des décisions en connaissance de cause peut varier considérablement d'un type de contenu à l'autre.

En principe, les utilisateurs devraient ne pas être obligés de s'identifier lorsqu'ils signalent ce qu'ils considèrent comme du contenu illicite, sauf si cette information est nécessaire pour déterminer la légalité du contenu (p. ex. vérifier la détention de droits de propriété intellectuelle). Cela est notamment le cas si leur sécurité risque d'être compromise ou si la divulgation de l'identité d'une personne peut avoir des conséquences juridiques. Les utilisateurs devraient être encouragés à faire parvenir leur notification par l'intermédiaire de signaleurs de confiance, lorsqu'il en existe, chaque fois qu'ils souhaitent conserver l'anonymat vis-à-vis des plateformes.

Cependant, **les notifiants devraient avoir la possibilité de fournir volontairement leurs coordonnées** dans une notification afin de permettre à la plateforme en ligne de leur demander des informations supplémentaires ou de les informer de la suite éventuellement prévue. Dans ce cas, le notifiant devrait recevoir un **accusé de réception** et un **message indiquant la suite donnée à la notification**.

L'accusé de réception évite non seulement au notifiant de devoir vérifier si sa demande a été suivie d'effet, mais peut aussi servir de preuve dans les procédures judiciaires ou extrajudiciaires conformément aux règles qui leur sont applicables.

3.3. Mesures proactives des plateformes en ligne

3.3.1. Mesures proactives et dérogation en matière de responsabilité

Compte tenu de l'importance de leur rôle et de leurs ressources ainsi que des responsabilités qui en découlent, les plateformes en ligne devraient ne pas se contenter de réagir aux signalements qu'elles reçoivent mais adopter également des **mesures proactives efficaces pour détecter et supprimer** les

contenus illicites en ligne. Qui plus est, pour certaines catégories de contenus illicites, il peut se révéler impossible d'atteindre pleinement l'objectif consistant à réduire le risque de dommages graves si les plateformes ne prennent pas ces mesures proactives.

La Commission estime que l'adoption de telles mesures proactives et volontaires **n'implique pas automatiquement que la plateforme en ligne perd le bénéfice de la dérogation en matière de responsabilité** prévue à l'article 14 de la directive sur le commerce électronique.

Premièrement, cette dérogation est réservée aux prestataires de services d'«hébergement» répondant aux conditions énoncées à l'article 14 de ladite directive, c'est-à-dire aux prestataires de services dont les activités consistent à stocker des informations à la demande de tiers et qui **ne jouent pas de rôle actif**, n'ayant pas la connaissance ni le contrôle de ces informations³³.

Le considérant 38 de la proposition de directive sur le droit d'auteur dans le marché unique numérique, que la Commission a présentée le 14 septembre 2016, dispose à cet égard: *«En ce qui concerne l'article 14 [de la directive sur le commerce électronique], il y a lieu de vérifier si le prestataire de services joue un rôle actif, notamment en optimisant la présentation des œuvres ou autres objets protégés mis en ligne ou en assurant leur promotion, indépendamment de la nature des moyens employés à cet effet.»*

En ce qui concerne plus précisément l'article 14 de la directive sur le commerce électronique, la Cour a indiqué, dans l'affaire L'Oréal contre eBay, que *«le simple fait [qu'une plateforme] en ligne stocke sur son serveur les offres à la vente, fixe les modalités de son service, est rémunéré[e] pour celui-ci et donne des renseignements d'ordre général à ses clients ne saurait avoir pour effet de [la] priver des dérogations en matière de responsabilité prévues par [l'article 14 de la directive sur le commerce électronique]»³⁴*. Selon la Cour, cet effet se produit toutefois *«[l]orsque, en revanche, [la plateforme en ligne] a prêté une assistance laquelle a notamment consisté à optimiser la présentation des offres à la vente en cause ou à promouvoir ces offres»³⁵*.

On peut en inférer que le simple fait qu'une plateforme en ligne adopte certaines mesures relatives à la fourniture de ses services d'une manière générale n'implique pas nécessairement qu'elle joue un rôle actif à l'égard des contenus individuels qu'elle héberge et qu'à ce titre elle ne saurait bénéficier de la dérogation. Selon la Commission, ces mesures peuvent, voire devraient, englober les mesures proactives qui seraient prises pour détecter et supprimer des contenus illicites en ligne, notamment lorsque lesdites mesures participent de l'application des conditions d'utilisation de la plateforme en ligne. Cette conception s'inscrit dans la logique de l'équilibre que la directive sur le commerce électronique cherche à instaurer entre les divers intérêts en jeu³⁶. Celle-ci rappelle, en effet, qu'il est dans l'intérêt de toutes les parties concernées d'adopter et d'appliquer des mécanismes rapides et

³³ Considérant 42 de la directive sur le commerce électronique. Voir arrêt Google France, points 114 et 120; arrêt du 12 juillet 2011, affaire C-324/09, L'Oréal contre eBay, point 113.

³⁴ Voir arrêt eBay, point 115.

³⁵ Voir arrêt eBay, point 116.

³⁶ Considérant 41 de la directive sur le commerce électronique.

fiables permettant de retirer les informations illicites et de rendre l'accès à celles-ci impossible³⁷. Bien qu'elle soustraie les plateformes en ligne à l'obligation générale de recherche active des faits³⁸, elle insiste également sur l'importance des mesures volontaires³⁹.

Deuxièmement, conformément à l'article 14 de la directive sur le commerce électronique, les prestataires de services relevant de cette disposition ne peuvent bénéficier de la dérogation en matière de responsabilité que s'ils remplissent **deux conditions**, à savoir: a) n'avoir pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'avoir pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ou b) dès le moment où ils ont de telles connaissances, agir promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

La Cour de justice a précisé que ces conditions visent *«toute situation dans laquelle [la plateforme en ligne concernée] prend connaissance, d'une façon ou d'une autre, de [faits et circonstances sur la base desquels un opérateur économique diligent aurait dû constater l'illicéité en cause]»*, ce qui comprend, outre le signalement émanant d'un tiers, la situation dans laquelle la plateforme *«découvre l'existence d'une activité ou d'une information illicites à la suite d'un examen effectué de sa propre initiative»*⁴⁰.

Par conséquent, en prenant des mesures proactives pour détecter ou supprimer des contenus illicites, une plateforme en ligne peut avoir connaissance d'activités ou d'informations illicites, ce qui pourrait lui ôter le bénéfice de la dérogation en matière de responsabilité prévue à l'article 14, paragraphe 1, point a), de la directive sur le commerce électronique. En pareil cas, la plateforme en ligne conserve toutefois la faculté d'agir promptement pour retirer les informations ou rendre l'accès à celles-ci impossible dès qu'elle en a connaissance. En agissant de la sorte, la plateforme en ligne peut conserver le bénéfice de la dérogation en matière de responsabilité au titre de l'article 14, paragraphe 1, point b). Par conséquent, la crainte de perdre le bénéfice de la dérogation en matière de responsabilité ne doit pas décourager ou empêcher l'application des mesures proactives et volontaires efficaces que la présente communication entend favoriser.

3.3.2. *Recours aux technologies pour détecter les contenus illicites*

Eu égard au volume du matériel relayé par les plateformes en ligne, ainsi qu'aux progrès technologiques réalisés dans les domaines du traitement de l'information et de l'intelligence artificielle, les **technologies de détection et de filtrage automatiques** constituent des outils de plus en plus importants pour lutter contre les contenus illicites en ligne. Beaucoup de grandes plateformes font désormais usage d'algorithmes d'appariement fondés sur un éventail de technologies qui vont du simple filtrage des métadonnées au hachage des contenus et à l'empreinte digitale numérique.

³⁷ Considérant 40 de la directive sur le commerce électronique.

³⁸ Article 15, paragraphe 1, de la directive sur le commerce électronique.

³⁹ Considérant 40 de la directive sur le commerce électronique.

⁴⁰ Voir arrêt eBay, points 120 et 121.

Dans la directive sur le commerce électronique, il est précisé que les dispositions sur la responsabilité ne font pas obstacle au développement et à la mise en œuvre effective de systèmes techniques de protection et d'identification ainsi que d'instruments techniques de surveillance rendus possibles par les techniques numériques⁴¹, cette mise en œuvre devant toutefois s'effectuer dans le respect des règles applicables du droit de l'Union et du droit national, notamment en ce qui concerne la protection de la vie privée et des données à caractère personnel et l'interdiction faite aux États membres d'imposer des obligations générales en matière de surveillance⁴².

Les législations sectorielles peuvent imposer aux plateformes en ligne de prendre des mesures, par exemple en matière de droit d'auteur, pour contribuer à la détection et à la suppression de contenus illicites et ce, même si elles peuvent bénéficier de la dérogation en matière de responsabilité prévue à l'article 14 de la directive sur le commerce électronique.

Plus généralement, l'utilisation et le développement de ces technologies sont encouragés, comme le Conseil européen en émet le souhait dans ses conclusions du 22 juin 2017⁴³, notamment lorsque des dommages graves risquent de survenir. Des outils et filtres automatiques peuvent être utilisés pour repérer les contenus potentiellement délictueux, et la recherche tant privée que publique progresse dans la mise au point de tels outils. Ainsi, dans le domaine du droit d'auteur, la reconnaissance automatique des contenus s'avère efficace depuis plusieurs années.

La **Commission soutient les nouvelles approches de recherche et d'innovation** allant au-delà de l'état actuel des techniques dans la perspective d'améliorer la précision des moyens techniques de détection des contenus illicites⁴⁴. Elle **encourage également le secteur privé à adopter effectivement les innovations pouvant contribuer à renforcer l'efficacité et l'efficacité des procédures de détection automatique.**

Dans la plupart des cas, les meilleures pratiques actuelles des entreprises consistent à utiliser des outils automatiques pour réduire la masse des contenus litigieux à soumettre à l'examen d'experts humains, qui peuvent avoir à se prononcer quant à eux sur le caractère illicite desdits contenus. Cette intervention humaine est, en général, un rouage important dans les mécanismes automatiques visant à déterminer l'illégalité d'un contenu donné, surtout dans les domaines caractérisés par des taux d'erreur élevés ou nécessitant une mise en contexte.

La Commission considère que les mesures proactives prises par les plateformes en ligne relevant de l'article 14 de la directive sur le commerce électronique afin de détecter et de supprimer les

⁴¹ Considérant 40 de la directive sur le commerce électronique.

⁴² Considérant 40 et article 15, paragraphe 1, de la directive sur le commerce électronique.

⁴³ <http://www.consilium.europa.eu/fr/press/press-releases/2017/06/22-euco-security-defence/>

⁴⁴ Les efforts de R&I actuellement déployés par les entreprises sont axés sur l'élaboration d'outils d'analyse permettant de mieux appréhender le langage naturel, les cascades d'informations sur les réseaux sociaux, l'identification des sources d'informations, les schémas de diffusion et les fausses identités. La Commission soutient également la R&I dans ce domaine en finançant des projets visant à mettre au point des outils de vérification automatique destinés à contrôler la véracité des contenus créés par les utilisateurs sur les réseaux sociaux. Ces outils peuvent être utiles pour repérer d'éventuelles informations mensongères dans les textes, les images ou les vidéos et contribuer au dépistage des fausses informations. Cependant, leurs capacités de fonctionnement actuelles ne leur permettent pas d'établir le caractère illicite de ces contenus.

contenus illicites qu'elles hébergent, y compris les outils automatiques et les outils destinés à éviter la remise en ligne de contenus supprimés précédemment, **ne les excluent pas en soi du bénéfice de la dérogation en matière de responsabilité.**

Ainsi, l'adoption de telles mesures n'implique pas nécessairement que la plateforme en ligne concernée joue un rôle actif la privant du bénéfice de cette dérogation. Dans les cas où l'adoption de telles mesures a pour conséquence que la plateforme en ligne a effectivement connaissance d'activités ou d'informations illicites, celle-ci doit agir promptement pour retirer les informations illicites en question ou rendre l'accès à celles-ci impossible de manière à satisfaire à la condition lui permettant de continuer à bénéficier de cette dérogation.

Les plateformes en ligne devraient mettre tout en œuvre pour détecter, circonscrire et éliminer de manière proactive les contenus illicites en ligne. La Commission encourage vivement les plateformes en ligne à user de mesures volontaires et proactives pour détecter et supprimer les contenus illicites et à renforcer leur coopération et leurs investissements dans le domaine des technologies de détection automatique ainsi que le recours à ces technologies.

4. SUPPRESSION DES CONTENUS ILLICITES

Il est dans l'intérêt de l'ensemble de la société que **les plateformes suppriment les contenus illicites le plus rapidement possible.** Dans le même temps, la suppression de ces contenus **ne doit pas faire obstacle aux poursuites ou autres mesures de suivi des infractions qui pourraient y être associées.** Le partage des informations probantes entre pouvoirs publics et plateformes en ligne est un aspect important du problème. La législation en préparation dans ce domaine devrait faciliter l'accès transfrontière aux éléments de preuves⁴⁵. La suppression des contenus illicites par les plateformes ne devrait pas avoir d'incidence sur les enquêtes ou les poursuites menées en vertu du droit de l'Union ou du droit national.

Il faut également prévoir des **garanties efficaces pour limiter le risque de suppression de contenus licites**, doublées d'un ensemble d'obligations de transparence utiles pour mieux rendre compte des opérations de suppression.

4.1. Promptitude des suppressions et notification des délits aux autorités répressives

La directive sur le commerce électronique impose aux plateformes en ligne d'agir «promptement» pour retirer les informations illicites après en avoir eu connaissance afin de pouvoir conserver le bénéfice de la dérogation en matière de responsabilité. Les implications pratiques de cette exigence dépendent des circonstances particulières de l'affaire, notamment du type de contenu illicite, de la précision du signalement et du préjudice qui aurait été causé.

Pratiquement, des types différents de contenus ne requièrent pas le même volume d'informations contextuelles pour déterminer la légalité d'un contenu donné. Par exemple, s'il est facile de

⁴⁵ Voir, pour plus d'informations, https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en et https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

déterminer la nature illicite d'un matériel pédopornographique, les propos diffamatoires demandent généralement une analyse prudente du contexte dans lequel ils ont été tenus.

Lorsque **les risques de dommages sont graves, comme dans les cas d'incitation à commettre des actes terroristes, la rapidité de suppression est particulièrement importante et peut être définie par des délais précis.**

Certains dispositifs volontaires, comme le code de conduite pour contrer les discours haineux illégaux diffusés en ligne, prévoient des objectifs indicatifs en matière de délais de suppression, en l'occurrence 24 heures dans la majorité des cas visés par ledit code de conduite.

L'automatisation totale de la suppression ou de la suspension de contenus peut être particulièrement efficace et devrait s'appliquer lorsque les circonstances ne laissent guère subsister de doute sur l'illégalité du matériel, notamment dans le cas de matériel dont la suppression est notifiée par les autorités répressives ou de contenus illicites connus qui avaient été supprimés antérieurement sous réserve des garanties visées au point 4.3.

En règle générale, **les suppressions déclenchées par des signalements émanant de signaleurs de confiance devraient faire l'objet d'une intervention plus rapide**, étant donné la qualité et la précision des informations fournies dans le signalement et le statut de fiabilité conféré aux signaleurs.

Lorsqu'un préjudice économique est à craindre en raison d'une atteinte aux droits de propriété intellectuelle, l'ampleur du préjudice éventuel peut être fortement corrélée à la rapidité de cette suppression.

Une communication claire, de la part des plateformes, sur les délais de traitement des demandes de suppression en fonction du type de contenu permettra d'apprécier plus facilement la promptitude de leur intervention et favorisera le respect de l'obligation générale de rendre des comptes.

En cas de doute, en particulier lorsque les plateformes en ligne éprouvent des difficultés à évaluer la légalité d'un contenu donné et s'il s'agit d'une décision pouvant donner lieu à contestation, elles pourraient avoir avantage à **consulter une tierce partie**. Ce rôle est joué par des organes d'autorégulation ou des autorités compétentes dans divers États membres. Cette coopération est vivement encouragée dans le cadre de la coopération renforcée entre les plateformes en ligne et les autorités compétentes.

Enfin, lorsqu'elles ont connaissance ou se trouvent en présence d'éléments attestant d'infractions pénales ou autres, **les plateformes en ligne devraient en référer aux autorités répressives** afin d'alerter les autorités concernées et de leur permettre d'enquêter et de poursuivre les auteurs de ces contenus ou les groupes terroristes ou criminels organisés ayant abusé de leurs services. Dans ce cas, elles doivent respecter les exigences légales applicables, parmi lesquelles le règlement (UE) 2016/679 sur la protection des données à caractère personnel⁴⁶. Pareille mesure pourrait s'imposer

⁴⁶ Article 6, paragraphe 1, point c), en liaison avec l'article 6, paragraphe 4.

également en cas d'offre et de vente de produits et de pratiques commerciales non conformes à la législation de l'Union.

Dans certains cas, la nécessité de coopérer avec les autorités répressives dans le cadre des enquêtes et des poursuites relatives aux infractions peut amener les plateformes à ne pas supprimer le contenu illégal en question, lorsqu'une enquête en cours l'exige, sous l'étroite surveillance des autorités nationales et dans le strict respect des règles nationales en matière de procédure pénale.

Les autorités répressives devraient se doter des moyens nécessaires pour donner aux signalements les suites qui s'imposent⁴⁷. Parmi les exemples de bonnes pratiques concernant les points de contact, on peut citer le portail SIRIUS⁴⁸ créé par Europol pour assister les États membres dans les enquêtes de contre-terrorisme en ligne, qui facilite notamment la coopération entre les plateformes et les autorités répressives de l'Union⁴⁹.

En application de l'article 14 de la directive sur le commerce électronique, les plateformes en ligne, si elles veulent bénéficier de la dérogation en matière de responsabilité, doivent supprimer promptement les contenus illicites dès qu'elles sont informées ou ont connaissance de leur existence. Une suppression particulièrement rapide est importante lorsqu'il s'agit de contenus illicites comportant des risques de dommages graves, comme les incitations à commettre des actes terroristes. Les délais et modalités de suppression des différentes formes de contenus illicites doivent figurer clairement dans les rapports de transparence.

La Commission poursuivra l'analyse de la question des délais de suppression fixes.

Les éléments de preuve relatifs à des infractions pénales qui ont été recueillis à l'occasion de la suppression de contenus illicites devraient être transmis aux autorités répressives, sous réserve du respect, notamment, des exigences du règlement (UE) 2016/679, singulièrement en ce qui concerne les motifs licites du traitement des données à caractère personnel.

4.2. Accroître la transparence

4.2.1. Transparence de la politique des plateformes en ligne en matière de contenu

La question de savoir si un contenu est licite ou non relève du droit de l'Union et du droit national. Parallèlement, les plateformes en ligne peuvent elles-mêmes considérer, dans leurs propres conditions d'utilisation, certains types de contenus comme indésirables ou répréhensibles.

⁴⁷ En vertu de l'article 15, paragraphe 2, de la directive sur le commerce électronique, «[l]es États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement».

⁴⁸ «Shaping Internet Research Investigations Unified System».

⁴⁹ Europol continuera de favoriser la création de nouveaux points de contact uniques en assurant des formations appropriées aux autorités répressives des pays qui ne disposent pas encore de tels points.

Les plateformes en ligne devraient préciser leur politique en matière de contenu dans leurs conditions d'utilisation et en informer clairement leurs utilisateurs. Il conviendrait non seulement d'y définir la politique retenue en matière de suppression de contenus ou de blocage de l'accès aux contenus mais aussi d'indiquer expressément les garanties prévues pour que les mesures prises à l'encontre de certains contenus illicites ne conduisent pas à des suppressions excessives. Les conditions d'utilisation des plateformes en ligne devraient notamment détailler, dans le cadre d'une transparence accrue des politiques générales des plateformes en matière de suppression, les possibilités dont disposent les utilisateurs pour contester les décisions de suppression. Cela devrait contribuer à réduire les risques d'effets négatifs sur le droit fondamental des utilisateurs à la liberté d'expression et d'information⁵⁰.

Les plateformes en ligne devraient fournir, **dans leurs conditions d'utilisation, des explications claires, faciles à comprendre et suffisamment précises sur leur politique en matière de contenu.** Ces explications devraient porter à la fois sur le traitement des contenus illicites et des contenus qui ne respectent pas les conditions d'utilisation de la plateforme. Toutes les restrictions imposées quant aux types de contenus autorisés sur une plateforme donnée devraient être clairement indiquées et portées à la connaissance de ses utilisateurs. Ces explications devraient comprendre également les procédures prévues pour contester les décisions de suppression, y compris celles qui procèdent de signalements émanant de signaleurs de confiance.

4.2.2. *Transparence des procédures de signalement et d'action*

Les rapports de transparence devraient évoquer également les *résultats* de l'application des politiques des plateformes en matière de gestion des contenus.

Les plateformes en ligne devraient **publier des rapports de transparence** contenant des informations suffisamment détaillées **sur le nombre et le type de signalements reçus et de mesures prises**, ainsi que **sur les délais de traitement** et la source des notifications⁵¹. Ces rapports devraient également contenir des informations sur les **contre-signalements** éventuels, ainsi que sur les suites données à ces contre-signalements. La Commission encourage la publication de ces informations à une fréquence régulière, au moins une fois par an.

Sans préjudice des différences spécifiques aux contenus concernés, ces rapports de transparence gagneraient à faire l'objet d'une **uniformisation** dans le marché unique numérique, qui permettrait un meilleur suivi, faciliterait l'agrégation des informations par des moyens électroniques et pourrait contribuer à lever les obstacles inutiles à la prestation transfrontière de services d'hébergement.

Il faudra veiller particulièrement à permettre aux petites plateformes en ligne et aux PME de fournir ces données de transparence, et toute activité connexe, comme l'uniformisation, devra impliquer un minimum de charges administratives.

⁵⁰ Si des données à caractère personnel sont traitées, les plateformes doivent prévoir des politiques transparentes en matière de respect de la vie privée, conformément à l'article 12 du règlement général sur la protection des données.

⁵¹ Rapports sur les enquêtes de leur propre initiative, les signalements émanant d'utilisateurs normaux, les signalements des services répressifs, etc.

La Commission continuera d'**explorer**, dans le cadre de dialogues structurés avec le secteur concerné, **les possibilités d'uniformisation** des procédures de notification et des rapports de transparence sur les systèmes de suppression et les résultats obtenus.

4.3. Garanties contre les suppressions excessives et l'utilisation abusive du système

Les actions rapides, comme le filtrage lors de la mise en ligne ou la détection automatisée à des fins de retrait rapide des contenus illicites, notamment en l'absence d'intervention humaine, peuvent influencer sur la justesse de la décision, au risque de supprimer des contenus licites. Il importe donc de veiller à l'existence de garanties suffisantes pour que les contenus retirés par erreur puissent être rétablis.

4.3.1. Contestation d'un signalement

D'une manière générale, les fournisseurs d'un contenu doivent **avoir la possibilité de contester une décision de suppression par la voie d'un contre-signalement**. Ce principe s'applique également lorsque la suppression du contenu est automatisée.

Par exemple, l'article 28 *bis* de la proposition visant à modifier la directive «Services de médias audiovisuels» prévoit que les États membres veillent à ce que des mécanismes de réclamation et de recours soient disponibles pour le règlement des litiges entre usagers et fournisseurs de plateformes de partage de vidéos concernant l'application des mesures appropriées à prendre par ces plateformes.

Si le contre-signalement fournit des motifs raisonnables de considérer que l'activité ou l'information signalée n'est pas illicite, **il incombe au prestataire de la plateforme de rétablir dans les meilleurs délais le contenu supprimé ou de permettre à l'utilisateur de le remettre en ligne, sans préjudice des conditions d'utilisation de la plateforme**.

La possibilité de contester les décisions devrait entraîner une baisse du nombre de suppressions injustifiées de contenus licites, tandis que les preuves documentaires pourraient être produites dans le cadre de mécanismes de règlement extrajudiciaire des litiges ou de procédures de recours contentieux.

Dans certaines circonstances, il convient de ne pas informer le fournisseur de contenus et/ou donner suite à un contre-signalement afin d'éviter d'empiéter sur les pouvoirs d'enquête dévolus aux autorités des États membres pour prévenir, détecter et poursuivre les infractions pénales, comme dans le cas de matériel pédopornographique.

Les plateformes en ligne devraient proposer des procédures de contre-signalement simples. Lorsqu'un contre-signalement est effectué, les plateformes en ligne devraient y répondre, en motivant le cas échéant une décision négative. Lorsque cette possibilité existe dans l'État membre concerné, les plateformes sont encouragées à autoriser le recours aux organes de règlement extrajudiciaire des litiges pour résoudre les litiges portant sur des contre-signalements.

4.3.2. Mesures contre les signalements et contre-signalements de mauvaise foi

Il peut arriver, dans le même temps, que les procédures de notification et d'action soient utilisées de manière abusive au moyen de procédés irréguliers ou de mauvaise foi⁵². Il convient de décourager fermement de telles pratiques en abaissant, par exemple, le niveau de priorité accordé aux signalements émanant d'une source présentant un taux élevé de signalements non valables ou faisant l'objet d'un grand nombre de contre-signalements, ou en retirant le statut de signaleur de confiance en fonction de critères bien établis et transparents. Ces politiques devraient également être décrites clairement dans les conditions d'utilisation des plateformes en ligne et figurer dans leurs rapports de transparence généraux dans un souci de responsabilisation vis-à-vis du grand public. Des mesures similaires devraient être établies à l'égard des contre-signalements abusifs.

5. PREVENIR LA REAPPARITION DES CONTENUS ILLICITES

Une fois détectés et retirés, les contenus illicites ne devraient plus réapparaître en ligne. Pour garantir le bon fonctionnement du système, il est essentiel d'assurer une prévention efficace et efficiente de cette réapparition en adoptant de bonnes pratiques et en prévoyant des garanties appropriées. Empêcher la diffusion de matériel illicite connu sur les plateformes demande une coopération plus étroite entre les prestataires de services en ligne, dans le strict respect des règles applicables du droit de la concurrence. Il importe également de renforcer la coopération entre les autorités répressives et les petites entreprises moins résilientes, sur lesquelles les auteurs d'infractions et autres personnes impliquées dans des activités délictueuses en ligne pourraient jeter leur dévolu si elles s'avèrent plus vulnérables.

5.1. Mesures contre la récidive

Pour éviter la réapparition de contenus émanant d'utilisateurs qui mettent ligne de manière répétée des contenus illicites de même nature, beaucoup de plateformes ont déjà instauré des mesures visant à empêcher la récidive, comme la suspension ou la suppression de comptes ou le «shadowbanning»⁵³.

Les plateformes en ligne devraient prendre des mesures de nature à dissuader les utilisateurs de mettre en ligne de manière répétée des contenus illicites de même nature et s'efforcer d'enrayer efficacement la diffusion de ces contenus.

Ce principe devrait également s'appliquer lorsque l'auteur de l'infraction est le même, que le contenu en question est de même nature et que, si cela est justifié, l'utilisateur a été rapidement informé des signalements reçus à son encontre et de l'imminence de la suspension ou suppression de son compte. Cela permettrait à l'utilisateur de contester la décision et faciliterait l'accès aux voies

⁵² Il semble que ces informations soient utilisées par les concurrents (*Notice and Takedown in Everyday Practice*, J Urban et al., UC Berkeley, 2016) et que la création automatisée de signalements est une pratique qui a été détournée pour renvoyer à des contenus créés artificiellement (Google Transparency report).

⁵³ Le «shadowbanning» consiste à bloquer l'accès d'un utilisateur à une communauté en ligne sans que ce dernier s'en rende compte.

de recours juridictionnelles contre la mesure, si le contrat conclu entre l'utilisateur et la plateforme ainsi que le droit applicable le prévoient. Dans ce type de cas également, tout traitement de données à caractère personnel doit respecter pleinement les règles en matière de protection des données y afférentes.

À nouveau, il convient de ne pas informer le fournisseur de contenus si cela risque d'empiéter sur les pouvoirs d'enquête dévolus aux autorités des États membres pour prévenir, détecter et poursuivre les infractions pénales, sous réserve de l'existence de la base juridique nécessaire.

5.2. Filtres automatiques contre la remise en ligne

Outre les technologies utilisées pour détecter les contenus potentiellement illicites, visées au point 3.3, d'autres outils peuvent en augmenter la fiabilité, comme le marquage par une empreinte digitale numérique ou le filtrage avec retrait définitif d'un contenu préalablement détecté et jugé illicite. Par conséquent, la Commission encourage fortement l'utilisation de tels outils moyennant des garanties comme la réversibilité et les exceptions évoquées ci-dessous.

C'est ainsi que le Forum de l'UE sur l'internet a créé la «base de données d'empreintes numériques» actuellement utilisée pour lutter contre les contenus terroristes, et l'idée fait son chemin dans le domaine du droit d'auteur ou du matériel pédopornographique, mais également dans le cas de produits dont les autorités répressives signalent qu'ils ne sont pas conformes à la législation applicable. Si ces pratiques donnent déjà de bons résultats, leur efficacité dépend des progrès à réaliser pour limiter les erreurs de détection et faciliter la prise de décisions en fonction du contexte, ainsi que des garanties fournies en matière de réversibilité.

Par exemple, se fondant sur les pratiques en matière de reconnaissance automatique des contenus dans le domaine du droit d'auteur, la proposition de la Commission sur le droit d'auteur dans le marché unique numérique range ces technologies, à condition qu'elles soient appropriées et proportionnées, parmi les moyens pouvant être utilisés, notamment, pour empêcher la présence de contenus ne faisant pas l'objet d'une licence sur les services en ligne concernés.

Les procédures automatiques de retrait définitif devraient comprendre des exceptions en fonction du contexte et lorsque les contenus retirés sont modifiés et mis en conformité avec les exigences légales ou autres. La portée et les délais applicables aux exceptions en fonction du contexte devraient tenir compte de la nature spécifique du contenu et de toute menace connexe pour la sécurité, ainsi que de la possibilité d'une suspension temporaire de ces contenus dans l'attente d'une analyse approfondie.

La Commission encourage fortement l'utilisation et le développement de technologies automatiques pour empêcher la réapparition de contenus illicites en ligne.

Lorsque des outils automatiques sont utilisés pour empêcher la réapparition de contenus illicites, une garantie de réversibilité devrait être prévue en cas de décision erronée, et l'utilisation et l'application de ces outils devraient figurer de manière transparente dans les conditions d'utilisation des plateformes.

L'accès aux bases de données utilisées pour apparier et détecter automatiquement les contenus illicites qui réapparaissent devrait être fourni à toutes les plateformes en ligne, sous réserve que le traitement effectué respecte la législation applicable en matière de protection des données à caractère personnel et de concurrence. Les politiques de respect de la vie privée appliquées par les entreprises devraient comprendre des informations transparentes sur le traitement des données à caractère personnel dans le cadre de ces bases de données.

Les plateformes en ligne devraient veiller à actualiser en permanence leurs outils pour prendre en compte tous les contenus illicites en suivant l'évolution des stratégies et des comportements des criminels et autres personnes impliquées dans des activités illicites en ligne. S'il s'agit d'outils servant à lutter contre les contenus à caractère terroriste, ils devraient être capables de prendre en compte des contenus nouveaux et historiques pour en assurer l'analyse et la suppression rapides. Ces contenus devraient être intégrés dans les outils transversaux, comme la base de données d'empreintes numériques évoquée plus haut (utilisée actuellement pour les contenus à caractère terroriste). Ces développements technologiques devraient être réalisés dans un esprit de coopération entre plateformes en ligne, autorités compétentes et autres parties prenantes, dont la société civile.

6. CONCLUSIONS

L'augmentation des contenus illicites hébergés par les plateformes en ligne cause de réels dommages dans la société, notamment des risques pour l'intégrité, la dignité et la santé de la population. À défaut de réaction appropriée, ces dommages s'étendront, de manière plus générale, à la confiance placée dans les services numériques et, en définitive, dans le marché unique numérique, moteur essentiel d'innovation, de croissance et d'emploi. Même si ces contenus sont créés et mis en ligne par des tiers, l'influence sans cesse grandissante des plateformes en ligne dans la société, en leur qualité de dépositaires de contenus et d'informations, accroît leur responsabilité à l'égard de leurs utilisateurs et de la société dans son ensemble. Elles devraient, dès lors, adopter une attitude volontariste dans l'élimination des contenus illicites et la prévention de leur réapparition, établir des procédures de notification et d'action opérantes, ainsi que des interfaces efficaces avec les tiers (tels que les signaleurs de confiance), et accorder une priorité particulière aux signalements effectués par les autorités répressives nationales. Lorsque les plateformes en ligne se prononcent sur le caractère illicite de contenus, dans le respect du droit, un système de contrepoids satisfaisant devrait être prévu.

La présente communication propose des orientations et, en tant que telle, ne modifie pas le cadre juridique applicable ni ne renferme de règles contraignantes. Elle vise principalement à fournir des indications aux plateformes sur les moyens dont elles disposent pour s'acquitter de leurs responsabilités afin de lutter contre les contenus illicites qu'elles hébergent. Elle vise également à généraliser les bonnes pratiques procédurales pour les différentes formes de contenus illicites et à encourager une coopération plus étroite entre les plateformes et les autorités compétentes. À ce titre, elle dessine les grandes lignes d'une approche européenne pour lutter contre les contenus illicites destinée aux plateformes en ligne, combinant la nécessité d'un retrait rapide et efficace des contenus illicites et la prévention et la poursuite des délits avec la préservation du droit à la liberté d'expression en ligne. Ces orientations compléteront et renforceront les dialogues sectoriels en cours.

Il convient de veiller particulièrement à ce que les plateformes en ligne de petite taille soient en mesure d'appliquer ces procédures, et de nombreux éléments de la présente communication ont été conçus en tenant compte de leurs besoins spécifiques. La Commission étudiera néanmoins d'autres moyens d'aider les petites plateformes à adopter et mettre en œuvre, elles aussi, les présentes orientations.

Le marché unique numérique exige une grande cohérence des réactions des pouvoirs publics à l'échelon transnational. Avec la présente communication, la Commission propose donc, dans un premier temps, des outils communs pour répondre au défi collectif de la suppression des contenus illicites.

La lettre d'intention du 13 septembre 2017 que le président de la Commission européenne a adressée au président du Parlement européen et au président du Conseil de l'Union européenne, afin de garantir un espace de justice et de droits fondamentaux basé sur la confiance mutuelle, annonçait de nouvelles mesures visant à assurer la détection rapide et proactive et la suppression des contenus illicites incitant à la haine, à la violence et au terrorisme. La présente communication constitue le premier volet de ces mesures. La Commission attend des plateformes en ligne qu'elles prennent des mesures rapides au cours des prochains mois, notamment dans le cadre des dialogues concernés, en particulier dans le domaine du terrorisme et des discours illicites d'incitation à la haine.

Elle poursuivra ses échanges et son dialogue avec les plateformes en ligne et les autres acteurs concernés. Elle suivra les progrès accomplis et déterminera si des mesures supplémentaires s'imposent pour assurer la détection rapide et proactive et la suppression des contenus illicites en ligne, telles que des mesures législatives complétant le cadre réglementaire en vigueur. Ces travaux s'achèveront au plus tard en mai 2018.