Observations formelles du CEPD 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

1. Introduction et contexte

- Les présentes observations formelles 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 (ci-après la «proposition»)[1], adoptée par la Commission européenne le 12 septembre 2018, sont émises par le Contrôleur européen de la protection des données (ci-après le «CEPD») en application de l'article 57, paragraphe 1, point g), et de l'article 58, paragraphe 3, point c), du règlement (UE) 2018/1725[2].

- La proposition vise à établir des règles uniformes pour les fournisseurs de services d'hébergement (ci-après les «FSH») qui proposent leurs services dans l'Union, quel que soit leur lieu d'établissement, afin de prévenir la diffusion, au moyen de leurs services, de contenus à caractère terroriste et de garantir leur suppression rapide.

- La proposition prévoit un ensemble d'obligations de vigilance incombant aux FSH et énonce diverses obligations pour les autorités compétentes des États membres en ce qui concerne l'application de la proposition. La proposition introduit notamment les mesures suivantes:

  – les FSH devraient prendre des mesures appropriées, raisonnables et proportionnées pour lutter contre la diffusion de contenus à caractère terroriste et protéger en particulier les utilisateurs contre ce type de contenus (article 3);
  – les FSH devraient supprimer les contenus à caractère terroriste ou en bloquer l'accès dans un délai d'une heure à compter de la réception d'une injonction de suppression émise par une autorité compétente d'un État membre (article 4);
  – les FSH devraient évaluer, sur la base des signalements adressés par les autorités compétentes des États membres ou par les organes de l'Union (tels qu'Europol), si les contenus identifiés dans le signalement violent les conditions commerciales des FSH et décider s'il convient de supprimer ces contenus ou d'en bloquer l'accès (article 5);
  – les FSH devraient prendre des mesures proactives pour protéger leurs services contre la diffusion de contenus à caractère terroriste, notamment au moyen d'outils automatisés afin d'évaluer les contenus stockés (article 6);

[1] Proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne, COM(2018) 640 final. Directive 2008/115/CE du Parlement et du Conseil du 16 décembre 2008 relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier.

[2] Règlement (UE) 2018/1725 du Parlement européen et du conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, JO L 295 du 21.11.2018, p. 39.

Adresse postale: rue Wiertz 60 – B-1047 Bruxelles
Bureaux: rue Montoyer 30
E-mail: edps@edps.europa.eu – Site web: www.edps.europa.eu
Tél. +32 22831900 – Fax +32 22831950

- les FSH devraient conserver les contenus qui ont été supprimés et les données connexes qui sont nécessaires aux fins des procédures de réexamen administratif ou de contrôle juridictionnel et de la prévention et de la détection d'infractions en relation avec le terrorisme ainsi que des enquêtes ou des poursuites y afférentes (article 7);
- les FSH devraient établir un mécanisme de réclamation pertinent permettant aux personnes dont les contenus ont été supprimés à la suite d'un signalement ou d'une mesure proactive d'introduire une réclamation auprès du FSH (article 10);
- les FSH devraient fournir des informations aux personnes dont les contenus ont été supprimés à la suite d'une injonction de suppression, d'un signalement ou d'une mesure proactive (article 11);
- les États membres devraient désigner une ou plusieurs autorités compétentes chargées d'émettre les injonctions de suppression, de détecter ou d'identifier les contenus à caractère terroriste et de les signaler aux FSH, de superviser la mise en œuvre des mesures proactives et de faire respecter les obligations prévues par la proposition sous peine de sanctions (article 17).

- Le CEPD comprend la nécessité de lutter contre la diffusion de contenus à caractère terroriste en ligne et de prévoir des obligations de vigilance pour les FSH à cet égard. Il soutient en outre les objectifs de la proposition. Il recommande des **améliorations qui pourraient être apportées** afin de **réduire de** manière significative **tout «conflit» éventuel avec les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel** et d'assurer in fine le respect sur le plan juridique de ces droits, tels qu'ils sont appliqués notamment par la Cour de justice de l'Union européenne (ci-après la «CJUE»).

- Le CEPD **prend note** de l'orientation générale adoptée par le Conseil sur la proposition le 6 décembre 2018[3], ainsi que de l'adoption du projet d'avis par la commission du marché intérieur et de la protection des consommateurs (IMCO) le 13 décembre 2018, du projet d'avis par la commission de la culture et de l'éducation (CULT) le 16 janvier 2019 et du projet de rapport émis par la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) le 21 janvier 2019[4].

- Les présentes observations formelles **portent essentiellement sur l'incidence éventuelle de la proposition sur les droits au respect de la vie privée et à la protection des données à caractère personnel**, eu égard aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte») et à l'article 16 du traité sur le fonctionnement de l'Union européenne (ci-après le «TFUE»). Toutefois, **notamment en ce qui concerne cette proposition, le CEPD note que le droit à la protection des données à caractère personnel est inextricablement lié à d'autres droits fondamentaux, tels que le droit à la liberté d'expression et d'information**[5],

[3] Procédure 2018/0331(COD), proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne – orientation générale.

[4] Les avis et le rapport des commissions du Parlement européen sur la proposition [documents liés à la procédure 2018/0331(COD)] sont disponibles à l'adresse suivante: http://www.europarl.europa.eu/committees/fr/draft-opinions.html?urefProcYear=2018&urefProcNum=0331&urefProcCode=COD&source=&linkedDocument=true&ufolderComCode=&ufolderLegId=&ufolderId=&ufolderId=#documents

[5] Voir Docksey, C., «Four fundamental rights: finding the balance», *International Data Privacy Law*, 2016, Vol. 6, nº 3, p. 203: «[D]ans certains contextes, tels que ceux de la surveillance de masse et de la réglementation indépendante, les droits au respect de la vie privée, à la protection des données et à la liberté d'expression fonctionnent de manière totalement complémentaire et se renforcent mutuellement.» En ce qui concerne l'incidence de la proposition sur les **droits fondamentaux liés au droit au respect de la vie privée et à la**

ainsi qu'aux principes généraux du droit de l'Union, tels que le principe de non-discrimination. La prise en considération de cette interrelation est conforme, entre autres, au règlement (UE) 2016/679 (ci-après le «RGPD»)[6], qui fait explicitement mention «des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques»[7].

2. Observations générales

2.1. Législation applicable en matière de protection des données

- Le CEPD note avec satisfaction que plusieurs dispositions de la proposition soulignent que le règlement assurera la protection des droits fondamentaux en jeu et que les FSH devraient toujours tenir compte des droits fondamentaux des utilisateurs[8]. À cet égard, le CEPD se félicite que le considérant 7 de la proposition souligne explicitement que le règlement assurera la protection des «droits au respect de la vie privée et à la protection des données à caractère personnel». Par souci de clarté, le CEPD recommande de **mentionner explicitement** dans le considérant précité **la législation applicable en matière de protection des données**, à savoir le RGPD et la directive (UE) 2016/680 (ci-après la «directive en matière de protection des données dans le domaine répressif»)[9]. Une formulation possible à cet égard est la suivante: «*La présente proposition ne porte pas préjudice aux règles applicables en matière de traitement des données à caractère personnel, notamment le règlement (UE) 2016/679 et la directive (UE) 2016/680.*»

2.2. Nécessité d'une définition claire des obligations imposées aux FSH dans la proposition

- Étant donné que les mesures à mettre en place au titre de la proposition (l'identification et la suppression des contenus à caractère terroriste) relèvent d'une «mission d'intérêt général», **toutes les mesures à prendre par les FSH en application de la proposition doivent être clairement décrites** par le législateur, et une **surveillance adéquate doit être assurée par des autorités publiques compétentes clairement identifiées**. Une telle approche contribuerait à répondre aux préoccupations concernant les pouvoirs répressifs dits «privatisés» (délégués à des entreprises privées, en l'occurrence les FSH) et serait conforme à la fois aux principes fondamentaux de «qualité de la loi»[10] et de

---

protection des données à caractère personnel, voir, entre autres, l'affaire *Tele2* (CJUE, C-203/15 et C-698/15, ECLI:EU:C:2016:970): «la conservation des données relatives au trafic et des données de localisation pourrait [...] avoir une incidence sur l'utilisation des moyens de communication électronique et, en conséquence, sur l'exercice par les utilisateurs de ces moyens de leur liberté d'expression, garantie à l'article 11 de la charte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 28)».

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

[7] Article 24, paragraphe 1, du RGPD.

[8] Voir notamment les considérants 7 et 17 ainsi que les articles 3 et 6 de la proposition.

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

[10] Dans l'arrêt *Digital Rights Ireland* (affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238), la CJUE a jugé que le **pouvoir d'appréciation du législateur** s'avère réduit lorsqu'il convient de limiter la portée des droits fondamentaux: «dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi

«sécurité économique» pour les opérateurs économiques (précisant les responsabilités juridiques des FSH).

- À cet égard, la proposition présente certaines lacunes, telles qu'elles sont exposées plus en détail dans les présentes observations formelles. Ainsi, la proposition ne contient pas de définition du terme «**données connexes**» que les FSH doivent conserver en application de l'article 7. À titre d'exemple, le considérant 20 précise que ces données «peuvent comprendre les données relatives aux abonnés, y compris notamment les données relatives à l'identité du fournisseur de contenus, ainsi que les données d'accès, y compris par exemple les données concernant la date et l'heure de l'utilisation par le fournisseur de contenus ou la connexion et la déconnexion du service, de même que l'adresse IP allouée par le fournisseur d'accès à l'internet au fournisseur de contenus».

- Le CEPD estime qu'une définition claire du terme «données connexes» est nécessaire afin d'éviter toute incertitude pour les FSH et de garantir parallèlement la sécurité juridique pour toutes les parties. Il recommande par conséquent de définir clairement le terme «données connexes», en fournissant une **liste exhaustive** des catégories de données qui devraient être conservées par les FSH[11].

- Le CEPD recommande également, dans le but de garantir un plus haut niveau de sécurité juridique pour les FSH, de **préciser et de clarifier** dans la proposition **les informations nécessaires et proportionnées pour garantir la suppression rapide des contenus à caractère terroriste par les FSH** que l'«autorité compétente» (à préciser comme il est recommandé au point 3.2.2 des présentes observations formelles) doit **inclure dans l'injonction de suppression** (informations «uniformisées» et facilement compréhensibles afin de repérer les contenus, comme l'adresse URL, et d'autres informations permettant l'identification et la suppression rapides des contenus à caractère terroriste).

---

lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci» (point 47). Répondant sur le fond à la question «Quelle est l'étendue du pouvoir d'appréciation (limité) du législateur de l'Union?», la CJUE a déclaré: «[l]a réglementation de l'Union en cause **doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause** et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données.» (point 54).
Concernant l'expression «prévue par la loi», voir également les conclusions de l'avocat général de la CJUE, 8 septembre 2015, avis 1/15 sur le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement des dossiers passagers, point 193: «Selon la jurisprudence de la Cour EDH, cette expression ["qualité de la loi"] exige, en substance, que la mesure en cause soit **accessible** et **suffisamment prévisible**, soit, autrement dit, qu'elle use des termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la CEDH.» (caractères gras ajoutés).
Plus récemment, sur ce point, voir l'arrêt de la Cour EDH, *Catt c. Royaume-Uni*, 24 janvier 2019.

[11] Étant donné que les obligations incombant aux FSH ne sont pas claires, ces derniers risquent d'être «incités» par la menace de sanctions prévues par le règlement [voir l'article 18, paragraphe 1, point e), qui renvoie à l'article 7] à collecter une **quantité excessive de données**, ce qui porterait préjudice à la protection des données à caractère personnel (ainsi qu'aux autres droits fondamentaux comme la liberté d'expression).

3. Remarques spécifiques

3.1. Définitions des termes «contenus à caractère terroriste», «diffusion de contenus à caractère terroriste» et «fournisseur de services d'hébergement»

- Le terme «**contenus à caractère terroriste**», défini à l'article 2, premier alinéa, point 5, englobe une ou plusieurs des informations suivantes: (a) «provoquent à la commission d'infractions terroristes, ou font l'apologie de telles infractions, y compris en les glorifiant, ce qui entraîne un risque que de tels actes soient commis»; (b) «encouragent la participation à des infractions terroristes»; et (c) «promeuvent les activités d'un groupe terroriste, notamment en encourageant la participation ou le soutien à un groupe terroriste au sens de l'article 2, paragraphe 3, de la directive (UE) 2017/541[12]». La proposition précise, à l'article 2, premier alinéa, point 4, que le terme «infractions terroristes» désigne les infractions définies à l'article 3, paragraphe 1, de la directive (UE) 2017/541. L'article 21 de la directive précitée dispose que «[l]es États membres prennent les mesures nécessaires pour faire rapidement supprimer les contenus en ligne constituant une provocation publique à commettre une infraction terroriste, visée à l'article 5»[13].
  Pour éviter toute incohérence entre la proposition et la directive susmentionnée, le CEPD recommande que la définition du terme «contenus à caractère terroriste» (à identifier et à supprimer par les FSH) soit **cohérente et étroitement alignée** dans les deux textes juridiques.

- Le CEPD se félicite que le considérant 9 énonce en particulier que les autorités compétentes et les FSH devraient tenir compte du contexte dans lequel ces contenus apparaissent et que les contenus diffusés à des fins pédagogiques, journalistiques ou de recherche devraient être protégés de manière adéquate. Le considérant précité précise également que l'expression d'opinions radicales, polémiques ou controversées dans le cadre du débat public sur des questions politiques sensibles ne devrait pas être considérée comme du contenu à caractère terroriste. Ces précisions, énoncées dans la proposition principalement dans le but de protéger le droit à la liberté d'expression, sont **également pertinentes du point de vue du respect de la vie privée et de la protection des données**, puisqu'elles «excluent» les catégories de contenus (et les «données connexes») qui ne seraient pas identifiées, supprimées et, in fine, conservées par les FSH.

- Le terme «**diffusion de contenus à caractère terroriste**» défini à l'article 2, premier alinéa, point 6, devrait également être aligné sur l'article 5 de la directive (UE) 2017/541. Ce dernier fait mention, contrairement au libellé actuel de la proposition (qui utilise la formulation peu claire «à des tiers»), de la mise à la disposition «*du public*» de contenus à caractère terroriste. Cette dernière formulation correspondrait mieux à l'objectif de la proposition, qui consiste à prévenir la diffusion en ligne de contenus à caractère terroriste. La même considération devrait être exprimée à l'article 2, premier alinéa, point 1, dans la définition du terme «**fournisseur de services d'hébergement**» (en remplaçant les termes «de tiers» par «du public»). Il résulterait, par exemple, de cette précision que les **services en nuage** qui ne rendent pas les contenus des utilisateurs accessibles à la diffusion (lesquels sont toutefois accessibles à des tiers), conformément aux objectifs de la proposition, ne relèveraient pas de son champ d'application.

[12] Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, JO L 88 du 31.3.2017, p. 6.
[13] Article 5 de la directive (UE) 2017/541(Provocation publique à commettre une infraction terroriste).

3.2. Injonctions de suppression

3.2.1. Prise de décisions dans un délai d'une heure à compter de la réception de l'injonction de suppression

- L'article 4, paragraphe 2, dispose que les FSH devraient **supprimer les contenus à caractère terroriste dans un délai d'une heure à compter de la réception de l'injonction de suppression** par l'autorité compétente. À cet égard, le CEPD note que l'analyse d'impact révèle que les contenus à caractère terroriste causent le plus grand tort dans les premières heures qui suivent leur «publication» en raison de la vitesse à laquelle ils sont diffusés en ligne. Le CEPD tient compte de cette considération relative à l'efficacité de la mesure (nettement moins efficace après une heure). Il fait toutefois observer qu'il convient également de noter qu'une suppression aussi rapide pourrait être difficile à exécuter[14], en particulier dans le cas des petits et moyens FSH, et priver les FSH de la possibilité d'effectuer un contrôle pertinent de l'injonction de suppression.

3.2.2. Authenticité des injonctions de suppression

- En outre, afin de permettre aux FSH d'exécuter dans les meilleurs délais la suppression visée au point 3.2.1. des présentes observations formelles, **une coopération harmonieuse et une interaction rapide entre les FSH et les autorités compétentes** sont indispensables. Par conséquent, le CEPD propose d'étudier, dans le cadre de la mise en œuvre «opérationnelle» de la proposition, l'application de **signatures numériques pour les injections de suppression transmises par voie électronique** et d'établir pour **chaque État membre une liste officielle et facilement accessible des autorités compétentes chargées d'adresser ces injonctions**. Ces mesures permettraient aux FSH de **vérifier** rapidement **l'authenticité** d'une injonction de suppression et de contacter les autorités compétentes en cas de doute sur l'injonction (autorité émettrice, contenu, modalités d'exécution, etc.). Ces précisions pourraient être ajoutées au considérant 14.

3.3. Mesures proactives

3.3.1. Mesures à prendre par les FSH afin de prévenir la diffusion de contenus à caractère terroriste en ligne selon une approche ciblée, «fondée sur les risques» et garantissant la responsabilité

- L'article 3 (Obligations de vigilance) dispose que les FSH «prennent des mesures appropriées, raisonnables et proportionnées [...] pour lutter contre la diffusion de contenus à caractère terroriste [...] [, en agissant] de manière diligente, proportionnée et non discriminatoire, en tenant dûment compte des droits fondamentaux des utilisateurs [...]». L'article 6, qui s'inscrit dans le cadre de l'ensemble des mesures à prendre par les FSH (avec les mesures relatives aux injonctions de suppression et aux signalements) pour se conformer aux «obligations de vigilance» énoncées dans la disposition «chapeau» de l'article 3, dispose que les FSH «prennent, s'il y a lieu, des **mesures**

[14] À cet égard, il apparaît à la page 8 de l'analyse d'impact accompagnant la proposition [SWD(2018) 408 final, 12.9.2018] que les contenus à caractère terroriste causent le plus grand tort dans les premières heures qui suivent leur parution en ligne. L'analyse d'impact ne fournit toutefois aucune preuve que l'application d'un délai aussi court soit effectivement réalisable. Au contraire, il est indiqué à la page 86 que les FSH ont souligné qu'un délai aussi court semblait impossible pour les petites entreprises.

proactives pour protéger leurs services contre la diffusion de contenus à caractère terroriste»[15]. Le CEPD souligne que l'article 6, paragraphe 1, fait également mention «du risque et du niveau d'exposition des FSH aux contenus à caractère terroriste» (approche fondée sur les risques) et recommande de rationaliser cette approche dans toute la proposition.

- À cet égard, le CEPD souligne, en tant que principe fondamental à respecter, que toute mesure limitant les libertés et droits fondamentaux devrait être nécessaire et proportionnée[16], ce qui présuppose qu'elle devrait être **aussi ciblée que possible**.

- En application de ce principe, le CEPD recommande d'introduire dans la proposition une obligation qui impose aux FSH, *avant* qu'ils ne mettent en place toute mesure proactive, de prendre les mesures suivantes:

  (i) réaliser et rendre publique une **évaluation des risques concernant le niveau d'exposition** aux contenus à caractère terroriste (également fondée sur le nombre d'injonctions de suppression et de signalements reçus);
  (ii) élaborer un **plan d'action** visant à lutter contre les contenus à caractère terroriste proportionnellement au niveau de risque cerné[17]. L'évaluation et le plan d'action susmentionnés serviraient également d'outils de renforcement de la **responsabilité** utiles à un examen périodique des mesures.

  Comme autre moyen de renforcer la responsabilité, les FSH devraient **rendre périodiquement compte** des mesures prises et du niveau résiduel de menace (exposition aux contenus à caractère terroriste).

3.3.2. Recours à des outils automatisés dans le cadre des mesures proactives et des garanties concernant l'utilisation de ces mesures

- Les considérants 16 et 18 et l'article 6, paragraphe 2, prévoient expressément que les mesures proactives peuvent inclure le **recours à des outils automatisés**. Le CEPD souligne que ces outils automatisés ne devraient être utilisés que de manière **prudente et ciblée**, sur la base des conclusions de l'évaluation des risques visée au point 3.3.1 des présentes observations formelles.

- Il insiste également sur le fait que les procédures envisagées dans la proposition conduisent dans certains cas, si ce n'est dans la plupart, à l'**identification de l'utilisateur** qui a mis en ligne les contenus à caractère terroriste (c'est le cas de la conservation des données relatives aux contenus supprimés qui doivent être stockées par les FSH en application de l'article 7 et éventuellement mises à la disposition des

[15] Le considérant 18 précise en outre que ces mesures proactives pourraient consister en des mesures visant à empêcher la remise en ligne de contenus à caractère terroriste qui ont été précédemment supprimés, par l'utilisation d'outils publics ou privés permettant de comparer ces contenus avec des contenus à caractère terroriste connus ainsi que par l'utilisation d'outils techniques fiables qui pourraient permettre d'identifier de nouveaux contenus à caractère terroriste.

[16] L'article 52, paragraphe 1, de la charte dispose que: «Toute limitation de l'exercice des droits et libertés reconnus par la présente charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui».

[17] L'analyse d'impact fait référence à l'«évaluation des risques» et au «plan d'action» dans le contexte de la mise en œuvre des mesures prévues à l'article 6 selon une approche fondée sur les risques. Au final, ces exigences n'ont toutefois pas été introduites dans la proposition.

services répressifs; de la mise en place, par l'utilisateur, d'un dispositif de réclamation en application de l'article 10; et de la fourniture d'informations sur la suppression par le FSH à l'utilisateur).

- À cet égard, le CEPD attire également l'attention sur le fait qu'il ne peut être exclu que les **mesures proactives prises par les FSH, y compris les outils automatisés, pour la reconnaissance et la suppression des contenus mis en ligne par les utilisateurs** puissent également être considérées comme des «décision[s] individuelle[s] automatisée[s], y compris le profilage[18]» au sens de l'article 22 du RGPD.

- Le CEPD rappelle que l'article 22, paragraphe 1, du RGPD prévoit, à l'égard des personnes concernées, une **interdiction générale de prise de décision individuelle fondée exclusivement sur un traitement automatisé**, produisant des effets juridiques les concernant ou les affectant de manière significative de façon similaire[19]. L'article 22, paragraphe 2, du RGPD prévoit toutefois des exceptions à cette interdiction générale et précise dans quels cas particuliers et sous quelles conditions une telle prise de décision est autorisée. En particulier, l'article 22, paragraphe 2, point b), du RGPD établit que le droit de l'Union ou des États membres peut autoriser une telle prise de décision lorsqu'il prévoit également des «**mesures appropriées**» pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée. À cet égard, le considérant 71 du RGPD souligne que ces «garanties appropriées» devraient, en tout état de cause, comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision.

- L'article 8, paragraphe 1, au titre des «obligations en matière de transparence», prévoit que les FSH devraient définir, dans leurs conditions commerciales, leur politique de prévention de la diffusion de contenus à caractère terroriste, «et y [joindre], **le cas échéant**, une **explication pertinente** du fonctionnement des mesures proactives, y compris le recours à des outils automatisés» (caractères gras ajoutés).

---

[18] L'article 4, premier alinéa, point 4, du RGPD définit le «profilage» comme suit: «toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.»
Le considérant 30 du RGPD précise que: «Les personnes physiques peuvent se voir associer, par les appareils, applications, outils et protocoles qu'elles utilisent, des **identifiants en ligne** tels que des **adresses IP** et des témoins de connexion ("cookies") ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes.» (caractères gras ajoutés).

[19] Étant donné que les outils automatisés, tels qu'ils sont envisagés dans la proposition, pourraient conduire non seulement à la suppression et à la conservation des contenus (et des données connexes) concernant la personne les ayant mis en ligne, mais également, in fine, à des enquêtes pénales à son encontre, ces outils **porteraient considérablement préjudice** à cette personne, portant atteinte à son droit à la liberté d'expression et présentant des risques non négligeables pour ses droits et libertés.
Les dispositions de l'article 22 du RGPD ont fait l'objet des «Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679» adoptées par le groupe de travail «Article 29» (à présent le comité européen de la protection des données) et disponibles à l'adresse suivante: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, lesquelles précisent à la page 21, que: «Même si un processus décisionnel n'a pas d'effet sur les droits juridiques des personnes, il pourrait quand même relever du champ d'application de l'article 22 s'il produit un effet équivalent ou qui affecte la personne concernée de manière significative de façon similaire.»

- En outre, l'article 9, paragraphe 1, dispose que les FSH qui recourent à des procédés automatisés prévoient des garanties efficaces et adéquates pour assurer l'exactitude et le bien-fondé des décisions prises en particulier pour supprimer des contenus ou en bloquer l'accès. L'article 9, paragraphe 2, précise que ces garanties consistent notamment en «**une surveillance et en des vérifications humaines**, **lorsque cela se justifie**, et à tout le moins lorsqu'une évaluation détaillée du contexte pertinent est nécessaire [...]» (caractères gras ajoutés).

- Compte tenu de ces garanties, le CEPD recommande de remplacer à l'article 8, paragraphe 1, et à l'article 9, paragraphe 2, les termes «le cas échéant» et «lorsque cela se justifie» par les termes «**en tout état de cause**» ou, à défaut, de supprimer ces termes[20].

- Le CEPD note également que, conformément à l'article 6, paragraphe 2, les FSH devraient soumettre un **rapport sur les mesures proactives qu'ils ont prises, y compris au moyen d'outils automatisés, à l'autorité compétente** chargée de surveiller la mise en œuvre des mesures proactives au titre de l'article 17, paragraphe 1, point c).

  Le CEPD recommande de préciser au considérant 18 de la proposition que les FSH devraient fournir aux autorités compétentes toutes les informations nécessaires sur les outils automatisés utilisés afin de permettre une surveillance publique approfondie de l'**efficacité** de ces outils et de veiller à ce que ces derniers **ne produisent pas de résultats discriminatoires, non ciblés, non spécifiques ou injustifiés**[21].

[20] D'un point de vue «technique», en ce qui concerne **les capacités et les limites de la reconnaissance automatisée des contenus**, qui doivent cependant être examinées compte tenu des spécificités des contenus illicites en jeu et de l'évolution des technologies (dites «de pointe»), voir *Mixed messages? The limits of automated media content analysis*, novembre 2017, CDT, p. 21 («tout recours à des outils automatisés d'analyse de contenus devrait s'accompagner d'un examen humain des résultats et des conclusions de l'outil»),
disponible à l'adresse suivante: https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf
Un autre point important souligné dans ce document est la nécessité de fournir une **définition claire, cohérente et précise du type de contenus** à identifier.

[21] Voir la *déclaration sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle*, adoptée lors de la 40e Conférence internationale des commissaires à la protection des données et de la vie privée, 23 octobre 2018, disponible à l'adresse suivante:
https://icdppc.org/wp-content/uploads/2018/10/20181023_ICDPPC-Declaration-AI_Adopted-FR.pdf
Voir notamment point 3, lettre c): «Il convient d'améliorer la transparence et l'intelligibilité des systèmes d'intelligence artificielle, l'objectif étant de permettre une mise en œuvre efficace, en particulier en procédant ainsi: **En rendant les pratiques des organisations plus transparentes, en particulier en mettant l'accent sur la transparence des algorithmes et la vérifiabilité des systèmes, tout en garantissant le sérieux des informations fournies**.»
En d'autres termes, le CEPD estime que la **responsabilité des FSH** doit être renforcée. Pour ce faire, un degré élevé de **transparence** est requis sur la manière dont le «retrait» éventuel des contenus mis en ligne est réalisé (orientations claires sur les circonstances dans lesquelles l'accès aux contenus est bloqué ou limité ou dans lesquelles les contenus sont supprimés). En tout état de cause, il semble communément admis que les décisions de retrait devraient faire l'objet d'une **vérification humaine** et que les FSH devraient fournir des **explications et des rapports utiles** sur le fonctionnement et l'efficacité des mesures envisagées. Une telle approche permettrait également de **vérifier et de s'assurer** que les mesures mises en place par les FSH: a) respectent strictement le principe de limitation de la finalité (elles ne sont pas utilisées à d'autres «fins»); b) ne produisent pas de résultats discriminatoires, non spécifiques ou injustifiés (compte tenu également de la «distribution» des faux positifs, pas seulement de leur quantité).

4. Conservation obligatoire des contenus et des données connexes par les FSH

- En vertu de l'article 7, les FSH seraient tenus de **conserver les contenus à caractère terroriste** (supprimés ou dont l'accès a été bloqué à la suite de l'une des trois séries de mesures prévues par la proposition, à savoir l'exécution d'injonctions de suppression, de signalements ou de mesures proactives) et les **données connexes**[22] aux fins des procédures de réexamen administratif ou de contrôle juridictionnel (en guise de garantie contre la suppression erronée) ainsi qu'aux fins de la prévention et de la détection d'infractions en relation avec le terrorisme ainsi que des enquêtes ou des poursuites y afférentes[23].

- Le CEPD note que l'imposition d'une telle obligation de conservation des données aux FSH nécessite que les entités privées soient tenues de conserver pendant six mois les données (y compris les données à caractère personnel relatives aux personnes qui mettent en ligne des contenus et aux infractions de nature pénale, les «infractions terroristes») à des fins répressives[24]. À cet égard, le CEPD rappelle que l'article 10 du RGPD dispose que le traitement des données à caractère personnel relatives aux infractions ne peut être effectué que sous le contrôle de l'autorité publique, *ou* si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des **garanties appropriées** pour les droits et libertés des personnes concernées.

- Étant donné que le traitement en question (conservation des contenus à caractère terroriste et des données connexes) *ne serait pas* effectué sous le contrôle d'une autorité officielle, le niveau approprié de garanties à assurer est un point essentiel. Le CEPD fait observer que l'article 7, paragraphe 3, dispose que les FSH devraient «veille[r] à ce que les contenus à caractère terroriste et les données connexes [...] fassent l'objet de garanties techniques et organisationnelles appropriées» et que ces «mesures garantissent que les contenus à caractère terroriste et les données connexes ne sont accessibles et traités qu'aux fins visées [...] et que la protection des données à caractère personnel concernées bénéficie du plus haut niveau de sécurité».

- Le CEPD rappelle que l'article 7 de la directive 2006/24/CE abrogée (ci-après la «directive sur la conservation des données»)[25] prévoyait, dans des termes analogues à ceux de la proposition, que «les données font l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites» et que «les données font l'objet de mesures techniques et organisationnelles appropriées afin de garantir que l'accès aux données

[22] En ce qui concerne la nécessité de définir le terme «données connexes», voir les considérations formulées au point 2.2. des présentes observations formelles.
[23] Voir le considérant 21.
[24] En particulier, le considérant 22 établit que: «Par souci de proportionnalité, il y a lieu de limiter la période de conservation à six mois afin de donner aux fournisseurs de contenus le temps suffisant pour engager la procédure de réexamen administratif ou de contrôle juridictionnel **et pour permettre aux autorités répressives d'avoir accès aux données pertinentes à des fins d'enquête et de poursuites en matière d'infractions terroristes**. **À la demande de l'autorité qui procède au réexamen, cette période peut toutefois être prolongée de la durée nécessaire lorsque la procédure de réexamen ou de contrôle juridictionnel est engagée mais non achevée à l'expiration de la période de six mois. Cette durée devrait être suffisante pour permettre aux autorités répressives de conserver les preuves nécessaires** en lien avec leurs enquêtes tout en assurant l'équilibre avec les droits fondamentaux concernés» (caractères gras ajoutés).
[25] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JO L 105 du 13.4.2006, p. 54.

n'est effectué que par un personnel spécifiquement autorisé». Toutefois, la CJUE a conclu, dans l'affaire *Digital Rights Ireland*, que la directive sur la conservation des données *ne* prévoyait *pas* des garanties suffisantes permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation ultérieure illicites de ces données[26].

- Le CEPD fait observer que l'on peut affirmer que la proposition, à l'instar de la directive sur la conservation des données, *ne* fixe *pas de* conditions matérielles et procédurales concernant **l'accès et l'utilisation ultérieure des données conservées** par les «autorités compétentes», comme l'exige la CJUE dans l'arrêt *Digital Rights Ireland*[27]. La simple mention, au considérant 23, que la proposition «n'a pas d'incidence sur les garanties procédurales ni sur les mesures d'enquêtes relatives à l'accès aux contenus et aux données connexes conservés à des fins d'enquête et de poursuites en matière d'infractions terroristes, qu'elles soient établies dans le cadre de la législation nationale des États membres ou de la législation de l'Union»[28] peut être considérée comme **insuffisante pour créer les conditions matérielles et procédurales requises pour l'accès et l'utilisation des données** à conserver obligatoirement par les FSH en exécution de l'obligation de conserver les données fixée dans la proposition.

- En outre, le CEPD n'est pas convaincu de **la nécessité et de la proportionnalité** de l'obligation de conservation des données incombant aux FSH aux fins de la prévention et de la détection d'infractions en relation avec le terrorisme ainsi que des enquêtes ou des poursuites y afférentes, étant donné que l'article 13, paragraphe 4, impose déjà aux FSH d'informer rapidement les autorités répressives compétentes de tout élément de preuve relatif à une infraction à caractère terroriste dont ils ont connaissance. En outre, l'article 13, paragraphe 4, de la proposition prévoit qu'en cas de doute, les FSH peuvent également transmettre ces informations à Europol, qui leur réservera un suivi approprié.

---

[26] Affaires jointes C-293/12 et -594/12, *Digital Rights Ireland*, voir notamment les points 54-55 et 65-67. Le CEPD attire plus particulièrement l'attention sur le point 55 («La nécessité de disposer de telles garanties est d'autant plus importante lorsque, comme le prévoit la directive 2006/24, les données à caractère personnel sont soumises à un **traitement automatique** et qu'il existe un risque important d'accès illicite à ces données») et le point 67 («L'article 7 de la directive 2006/24 [...] ne garantit pas que soit appliqué par lesdits fournisseurs un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles, mais autorise notamment ces fournisseurs à tenir compte de considérations économiques lors de la détermination du niveau de sécurité qu'ils appliquent, en ce qui concerne les coûts de mise en œuvre des mesures de sécurité. En particulier, la directive 2006/24 ne garantit pas la destruction irrémédiable des données au terme de la durée de conservation de celles-ci.») (caractères gras ajoutés).

[27] Voir l'arrêt *Digital Rights Ireland*, points 61-62, «[...] quant à l'accès des autorités nationales compétentes aux données et à leur utilisation ultérieure, la directive 2006/24 ne contient pas les conditions matérielles et procédurales y afférentes. L'article 4 de cette directive, qui régit l'accès de ces autorités aux données conservées, ne dispose pas expressément que cet accès et l'utilisation ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci, mais il **se borne à prévoir que chaque État membre arrête la procédure à suivre et les conditions à remplir** pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité. (62) En particulier, la directive 2006/24 ne prévoit aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi. Surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales. Il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles limitations.» (caractères gras ajoutés).

[28] Voir le libellé similaire à l'article 4 (*Accès aux données*) de la directive 2006/24/CE.

- À la lumière de ce qui précède, le CEPD recommande de **réexaminer la proposition d'obligation de conservation des données** incombant aux FSH en ce qui concerne les contenus à caractère terroriste et les données connexes, visée à l'article 7, paragraphe 1, point b).

5. Dispositif de réclamation

- L'article 10 dispose que les FSH établissent des mécanismes efficaces et accessibles permettant aux fournisseurs de contenus dont les contenus ont été supprimés ou dont l'accès a été bloqué d'introduire une réclamation contre l'action du FSH. Conformément à l'article 10, paragraphe 2, les FSH examinent dans les meilleurs délais la réclamation et informent le fournisseur de contenus des conclusions de leur examen.

- Le CEPD se félicite de l'introduction d'un **dispositif de réclamation**, étant donné qu'il pourrait contribuer à renforcer les garanties offertes aux personnes qui mettent en ligne des contenus contre les suppressions erronées. Il recommande toutefois d'insérer à l'article 10 un **délai pour la prise d'une décision par le FSH** sur la réclamation, ainsi que de préciser que le dispositif de réclamation à mettre en place par le FSH est **sans préjudice des lois et procédures applicables** des États membres (et sans préjudice des recours prévus par la législation applicable en matière de protection des données).

Bruxelles, le 12 février 2019

(signé)

Giovanni BUTTARELLI