COMMISSION
EUROPÉENNE

Bruxelles, le 12.9.2018
SWD(2018) 409 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DE L'ANALYSE D'IMPACT

accompagnant le document:

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} - {SEC(2018) 397 final} - {SWD(2018) 408 final}

Résumé de l'analyse d'impact

Analyse d'impact relative à la prévention de la diffusion de contenus à caractère terroriste en ligne

A. Nécessité d'une action

Pourquoi? Quel est le problème?

La prolifération de contenus à caractère terroriste en ligne reste un sujet de préoccupation important et urgent pour la société et la classe politique. En dépit de plusieurs mesures non réglementaires, les services d'hébergement en ligne continuent d'être utilisés pour diffuser des contenus à caractère terroriste.

Quels sont les résultats escomptés de l'initiative?

L'initiative a pour finalité de susciter une plus grande confiance dans l'environnement en ligne dans le marché unique numérique en limitant la disponibilité de contenus à caractère terroriste en ligne, tout en assurant un niveau de sécurité élevé aux citoyens de l'Union européenne. En particulier, elle vise à améliorer l'efficacité des mesures visant à détecter et à supprimer les contenus à caractère terroriste, tout en renforçant la transparence et la responsabilité des fournisseurs de services d'hébergement. Les mesures visent également à renforcer les capacités des autorités compétentes à lutter contre les contenus à caractère terroriste en ligne, à se prémunir contre le risque de suppression, par erreur, de contenus légaux, et à garantir une protection appropriée des droits fondamentaux.

Quelle est la valeur ajoutée d'une action à l'échelle de l'Union européenne?

La plupart des plateformes en ligne œuvrent au-delà des frontières et offrent un accès à leurs contenus indépendamment du lieu où se trouvent les utilisateurs ou les fournisseurs d'informations. Les États membres ont légiféré dans le domaine de la suppression des contenus illicites en ligne, mais la nécessité d'assurer la sécurité du public à l'échelle nationale doit être pondérée par la libre prestation de services et la liberté d'établissement conformément aux règles du marché unique.

Un cadre disparate de règles nationales fait son apparition ou risque de prendre de l'ampleur; une telle évolution mettrait en péril l'exercice effectif de la liberté d'établissement ou de la liberté de fournir des services dans l'UE, tout en limitant l'efficacité de la lutte contre les contenus à caractère terroriste en ligne, car cela alourdirait les coûts de mise en conformité pour les entreprises.

Compte tenu de la nature des services en question et de la fragmentation émergente du marché intérieur, une action à l'échelle des seuls États membres ne permet pas d'apporter une réponse efficace à la question de la limitation de la disponibilité des contenus illicites en ligne.

B. Les solutions

Quelles options législatives et non législatives ont été examinées? Y a-t-il une option privilégiée? Pourquoi?

En plus du scénario de base, l'analyse d'impact a examiné trois options suivant une logique d'intervention similaire, mais présentant des degrés d'intensité divers sur le plan de l'efficacité et de l'incidence sur les droits fondamentaux. Les options reposent sur les éléments suivants:

Des dispositions visant à **harmoniser les procédures de suppression ou de blocage de l'accès aux contenus à caractère terroriste** à la suite d'une injonction de suppression émise par une autorité nationale. Pour que les procédures puissent fonctionner, l'harmonisation nécessite également l'adoption d'une **définition commune de ce qu'on entend par «contenus à caractère terroriste en ligne»** (différentes définitions sont examinées dans les trois options), ainsi que de faire la clarté en ce qui concerne le **recours judiciaire** que peuvent intenter les fournisseurs de services d'hébergement et les fournisseurs de contenus contre les injonctions de suppression (élément commun à toutes les options).

Des dispositions visant à assurer des **procédures et processus transparents d'information** des autorités et de la Commission (similaires dans toutes les options). Ces dispositions renforceraient la responsabilité et amélioreraient la confiance dans le processus de modération des contenus tout en soutenant les décideurs

politiques et les autorités nationales dans leur lutte contre les contenus à caractère terroriste et en permettant aux utilisateurs de mieux comprendre la manière dont les fournisseurs de services d'hébergement appliquent leur politique de gestion des contenus.

La coopération entre les autorités nationales et Europol (à des degrés d'intensité divers selon les options) renforcerait leurs capacités à lutter collectivement contre les contenus à caractère terroriste, en évitant les doubles emplois, et réduirait la complexité et les coûts de la collaboration entre les fournisseurs de services d'hébergement et les autorités nationales lorsqu'ils proposent leurs services au-delà des frontières.

De plus, des dispositions permettant de s'assurer que, dans les cas où des entreprises sont exposées à des contenus à caractère terroriste, les fournisseurs de services d'hébergement mettent en place des **mesures appropriées et proportionnées visant à détecter activement les contenus à caractère terroriste** (exigences différentes en fonction des options).

Des garanties (communes à toutes les options) et d'autres dispositions visant à s'assurer que les mesures adoptées pour détecter et supprimer les contenus à caractère terroriste ne mènent pas à la suppression, par erreur, de contenus légaux, et respectent les droits fondamentaux.

Des dispositions visant à **s'assurer que les mesures sont applicables** (communes à toutes les options), y compris la désignation de représentants légaux d'entreprises de pays tiers, permettant d'établir des points de contact et de veiller à ce que les États membres mettent en place un ensemble de sanctions cohérent.

Le rapport présente une combinaison des mesures considérées comme étant les plus efficaces dans la lutte contre les contenus à caractère terroriste en ligne. Il présente également une évaluation des avantages des différents éléments sur le plan de leur efficacité.

L'analyse d'impact conclut que l'inclusion de mesures telles qu'une définition précise de ce qu'on entend par «contenus à caractère terroriste», d'exigences relatives à la suppression des contenus faisant l'objet d'une injonction de suppression dans un délai d'une heure et à l'évaluation des signalements tant d'Europol que des États membres, ainsi que d'exigences pour les fournisseurs de services d'hébergement exposés à des contenus à caractère terroriste d'adopter des mesures proactives afin de détecter tout nouveau contenu à caractère terroriste et d'éviter la remise en ligne de matériel connu, ainsi qu'un ensemble de garanties solides contre la suppression, par erreur, de contenus légaux, et des obligations en matière de transparence, seraient plus efficaces pour atteindre les objectifs de cette politique.

Qui soutient quelle option?

Les fournisseurs de services d'hébergement sont généralement favorables à l'option fondée sur le scénario de base et considèrent qu'il conviendrait, avant toute chose, d'évaluer tous les effets des efforts non réglementaires. Si un instrument juridique doit être adopté, leur préférence va à une intervention ciblée sur des besoins spécifiques présentant un intérêt public particulier.

Les États membres reconnaissent la nécessité de nouvelles mesures de soutien (à savoir une évolution continue du scénario de base) et sont en faveur d'une intervention ciblée sur les contenus à caractère terroriste. Les États membres ont particulièrement mis en exergue la nécessité d'adopter une définition commune de l'expression «contenus à caractère terroriste», l'obligation de prendre des mesures en cas de signalement, la nécessité de prendre des mesures proactives, mais aussi d'assurer la transparence et d'adopter des mesures permettant d'avoir accès au contenu supprimé à des fins répressives. Le Conseil européen a demandé à la Commission de «présenter une proposition législative visant à améliorer la détection et la suppression des contenus incitant à la haine et à la commission d'actes terroristes.»

La société civile représentant les droits numériques et les milieux universitaires se sont prononcés en faveur de l'évolution du scénario de base. Ils ont recommandé la prudence sur certains points, y compris dans les options réglementaires, en particulier en ce qui concerne les mesures proactives et les effets sur les droits fondamentaux. Des particuliers ont partagé ces préoccupations dans leurs réponses à la consultation publique. Un échantillon représentatif de citoyens répondant à un Eurobaromètre sur la question a plaidé en faveur de mesures supplémentaires à l'échelle de l'Union pour lutter contre les contenus illicites en ligne.

C. Coûts et bénéfices de l'option privilégiée

L'analyse d'impact détaille les coûts et bénéfices des mesures figurant dans chaque option. Elle conclut que l'option 3 est la plus efficace. L'option stratégique contribuerait dans une large mesure à atteindre les objectifs

stratégiques et serait particulièrement intéressante compte tenu de l'ampleur et de la portée du problème. Certes cette option devrait avoir les effets économiques les plus importants en ce qui concerne les coûts et la charge administrative supplémentaire attendus, mais elle devrait aussi offrir les avantages les plus importants.

D. Suivi

Quand aura lieu le réexamen de la stratégie?

Un programme détaillé de suivi des réalisations, résultats et effets de la législation sera élaboré afin d'étayer l'évaluation. Le suivi reposera principalement sur les informations fournies par les États membres, qui auront été rassemblées par les autorités compétentes dans l'exercice de leurs fonctions, et complétées par des rapports de transparence accessibles au public. D'autres informations, en particulier sur les mesures proactives, seront fournies par les fournisseurs de services d'hébergement dans le cadre de leurs obligations d'information. Dans toutes les options, ce suivi sera complété par des recherches visant à mieux comprendre la diffusion de contenus illicites en ligne, ainsi qu'à suivre l'évolution technologique en matière d'outils informatiques permettant la suppression de contenus illicites.