This document has not been adopted or endorsed by the European Commission. Any possible measures indicated in this paper are the preliminary elements being considered by the Commission services, they do not preclude the measures to be finally considered in the Impact Assessment and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the Member State or entity to which it is addressed for discussions and for the preparation of the Impact assessment and may contain confidential and/or privileged material.

IMPACT ASSESSMENT ON ILLEGAL CONTENT ONLINE
STAKEHOLDER CONSULTATION:
MEMBER STATES

Introduction:

Following the initial discussion with Member States at the EU Internet Forum (EUIF), the Commission would like to get more detailed views on possible actions to more effectively tackle terrorist content online as part of the ongoing work on the Impact Assessment on Illegal Content Online. These views will complement the Open Public Consultation (OPC, available **here**), as well as the data collection exercise based on the table of indicators.

The Commission started work on an impact assessment outlining potential problems, objectives and options in the attached Inception Impact Assessment (IIA). As part of the options to be considered, the Commission will analyse the current situation (baseline scenario) as well as actions to reinforce the voluntary measures as well as possible sector-specific legislation (including in particular on terrorism content online) as well as horizontal legislation applicable to all types of illegal content.

The measures presented in the Inception Impact Assessment[1]are initial ideas, and additional actions and options could be considered. The actions to be undertaken would be mainly addressed to online platforms, but could also require further action by Member States.

Member States are kindly requested **to reply to the questions below and provide any additional considerations in writing by 13 June 2018**. The results of this questionnaire will be presented and discussed at the **forthcoming meeting on 15 June**. In parallel, the European Commission's Directorate-General for Communications Networks, Content and Technology convened its expert group under the eCommerce Directive also feeding into the work of the impact assessment.

[1] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1183598_en

Questions

I. Problem and baseline scenario

1. What are the **provisions, arrangements etc under national law addressing the removal of terrorist content[2] for preventive purposes** (e.g. do you have duty of care provisions[3], specific notice and action procedures, provisions on transparency of companies' actions in relation to the removal of terrorist content, provisions on safeguards, etc.)? Please indicate below – where relevant – the applicable laws or other legal documents.

Notice and action procedures	Conformément à l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), les hébergeurs de données peuvent voir leur responsabilité engagée à raison du stockage de contenus manifestement illicites s'ils en ont eu connaissance et n'agissent pas promptement pour les retirer ou en rendre l'accès impossible. Les hébergeurs et les fournisseurs d'accès à Internet ne sont pas soumis à une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites. Ils doivent par contre mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance les contenus les plus préjudiciables : apologie des crimes contre l'humanité, provocation à la commission d'actes de terrorisme et apologie, incitation à la haine, pornographie enfantine, incitation à la violence et atteintes à la dignité humaine.

[2] For the purpose of this questionnaire, "terrorist content" is defined as in the Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final). https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[3] See recital 48 of the Directive on electronic commerce

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031

Transparency rules	Ils ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites qui leur sont signalées dans ces domaines et qu'exercent les utilisateurs de leurs services, et, d'autre part, de rendre publics les moyens qu'ils consacrent à la lutte contre ces activités.
Safeguards	

Do you have **specialised entities that notify/refer terrorist content** to hosting service providers? What is the **legal basis and benchmark for notification/referral** (illegality of content, terms of service of hosting service provider)?

L'article 6-1 de la LCEN prévoit un dispositif permettant à une autorité administrative spécialement désignée de prescrire aux hébergeurs, aux fournisseurs d'accès à Internet et aux moteurs de recherches, respectivement des mesures de retrait, de blocage et de déréférencement des contenus pédopornographiques, des contenus faisant l'apologie du terrorisme et des contenus provoquant à des actes terroristes.

L'autorité administrative désignée est l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (sous-direction de la lutte contre la cybercriminalité / direction centrale de la police judiciaire/plateforme PHAROS).

Do you consider them **sufficient** in terms of preventing accessibility of terrorist content? What are the limitations?

Les mesures de retrait, lorsqu'elles sont exécutées, sont efficaces par définition. Les taux de retrait sont variables selon les hébergeurs. Les hébergeurs français sont globalement très réactifs. Des difficultés variables sont par contre rencontrées avec les hébergeurs localisés dans d'autres pays.

Le retrait des contenus n'empêche pas leur remise en ligne chez d'autres hébergeurs. C'est pourquoi, au-delà des mesures de retrait, il est important de poursuivre les travaux engagés avec les prestataires techniques pour promouvoir l'**utilisation d'outils de détection automatisée des contenus illicites et le partage des bases de données des signatures numériques des contenus déjà connus**. D'autre part, l'i**dentification des auteurs** des diffusions, quand elle est possible, doit rester une priorité d'action dans la mesure où l'exercice de poursuites judiciaires constitue un facteur de dissuasion.

2. Do you consider that the **amount of terrorist content online** in the last [two] years has overall

	Decreased substantially
X	Decreased
	Continued at the same level
	Increased
	Increased substantially

Please indicate the basis for your assessment. What do you think has contributed to this trend?

Le nombre de contenus signalés à la plateforme nationale de traitement des contenus illicites de l'Internet (PHAROS) dans le domaine du terrorisme avait considérablement augmenté en 2015 dans le contexte des attentats subis par la France. En 2016 et en 2017, en baisse, il est toutefois resté très important.

Il doit être pris en compte le fait que ces données reflètent non seulement le nombre de contenus terroristes diffusés sur Internet, mais également la sensibilité du public à ces contenus.

Nombre de signalements reçus par la plateforme dans le domaine du terrorisme :

- en 2014 : 1675
- en 2015 : 31 305
- en 2016 : 11 422
- en 2017 : 6 263

Nombre de contenus identifiés après recoupements :

- en 2014 : 716
- en 2015 : 16 558
- en 2016 : 7 773
- en 2017 : 4 482

3. Do you see a **risk that removal by companies** on their own initiative could **interfere with investigations or intelligence gathering**? What would be the **mitigating measures** necessary to address any such risks?

Ce risque ne peut être écarté. L'interférence pourrait être atténuée dans une certaine mesure par les signalements que les prestataires techniques doivent adresser aux autorités et par la mise en place obligatoire de dispositifs techniques de "délestage" (espaces permettant à des hébergeurs de répliquer des contenus dans leur état d'origine

sans qu'ils soient visibles par le public, permettant aux services de police de réaliser des constatations).

4. Do you see a risk of **erroneous removal** by platforms of legal content (e.g. removal of content misidentified as illegal, removal of content disseminated for research, educational or journalistic purposes, "over-removal")? Are you aware of **any cases** of over-removal? What would be the **mitigating measures** necessary to address any such risks?

Ce risque est patent, les opérateurs privés n'ayant pas la légitimité des autorités administratives et judiciaires pour apprécier le caractère illicite des contenus qu'ils détectent ou qui leur sont signalés. En outre, le risque de l'engagement de leur responsabilité juridique ou de la dénonciation médiatique de leur inaction est de nature à les inciter à supprimer des contenus licites.

La sécurité juridique des opérateurs démontrant leur volonté de lutter efficacement contre les contenus illicites est de nature à favoriser la liberté de publication des contenus licites.

Une sensibilisation des entreprises sur la législation en vigueur (apologie du terrorisme ou d'une infraction pénale, contenus pédo-pornographiques et diffamations/injures notamment) serait souhaitable afin de prévenir des retraits de contenus qui ne poseraient pas de difficulté.

II. Non regulatory options: reinforcing voluntary action

1. Do you think that the work under the **EUIF** as reinforced and complemented by the **Recommendation** is **sufficient** action at EU level to effectively tackle terrorist content online?

L'action multilatérale engagée au niveau européen a ciblé avec pertinence les enjeux et les moyens de la lutte contre les contenus terroristes sur Internet. Elle gagnerait à être complétée par des actions bilatérales visant à faire adopter par les fournisseurs de service les moins vertueux les pratiques d'autres opérateurs. Toutefois, l'expérience opérationnelle montre qu'il y a des limites au dialogue : obtenir des plus petites entreprises la même détermination à lutter contre les contenus terroristes restera difficile, compte tenu de leur nombre, de la disparité de leurs moyens et de leur faible propension à se faire connaître des autorités compétentes des Etats européens. Le récent déplacement de la FR, UK et l'Allemagne pour rencontrer les opérateurs illustre par ailleurs les limites à la coopération (Wordpress s'est montré peu réceptif aux messages passés par les trois délégations).

Par ailleurs, l'action engagée dans le domaine du retrait des contenus doit être complétée par la poursuite des travaux engagés dans le domaine du recueil de la preuve numérique (voir au I-1). Il est nécessaire d'améliorer et de simplifier les outils juridiques permettant l'obtention transfrontalière des preuves numériques et d'inciter les opérateurs techniques, notamment américains, à répondre favorablement aux demandes de données qui leur sont directement adressées par des enquêteurs européens. Dans ce domaine, les pratiques des opérateurs sont disparates et les meilleures pratiques peuvent être érigées en modèles pour les opérateurs les moins coopératifs.

2. Do you consider that the **EUIF's work should be further developed** in order to reinforce action at EU level to tackle terrorist content online e.g. through a Memorandum of Understanding in which companies and possibly Member States would sign up to concrete commitments (see possible measures below)?

Cf point 1) sur les limites du cadre collaboratif.

3. Which of the following **possible elements** should in your view be addressed and further developed within a voluntary approach? Please indicate the need from a scale from 1 (unnecessary) to 5 (very necessary)

	More specific objectives for companies' actions (e.g. request a certain percentage of content taken down within a certain time limit) Il faut partir du principe que 100% des contenus signalés par les autorités publiques doivent être retirés. [redacted]
5	Stronger commitments in terms of internal processes and resource allocation (e.g. to have certain procedures in place, conduct risk assessments and establish

	mitigating procedures, content of Terms of Service, training, capacity to detect content in different languages)
5	Standardised working arrangements between companies, law enforcement and Europol to enhance understanding of how platforms are abused, to improve referral mechanism, avoiding unnecessary duplication of efforts, facilitating requests from law enforcement agencies in relation to criminal investigations[4].
5	Stronger commitment on specific proactive and preventive measures (i.e. further development and participation in industry-led schemes, such as the database of hashes developed in the context of the EUIF)
4	More detailed requirements on transparency and reporting
4	More detailed requirements to companies on safeguards against over-removal
5	Establishment of an external audit/monitoring mechanism
5	Establishment of contact points, both in companies and Member States, to facilitate referrals (and feedback) and requests from law enforcement authorities in relation to criminal investigations.
5	*Additional support (e.g. by Europol) to referral capacities in Member States* – Besoins variables selon les États membres et les infrastructures qu'ils ont mises en place pour centraliser et signaler les contenus illicites.

4. What other additional measures could be developed within a reinforced voluntary approach?

L'action pourrait être étendue aux contenus relevant de la haine en ligne (incitation à la haine pour des raisons religieuses ou raciales notamment), qui créent un climat favorable aux discours terroristes.

5. Which further actions could be taken to secure participation from those **companies** who have **not engaged**?

Voir 6 ci-dessous

6. Which further actions could be taken to **support small companies** and start-ups in tackling terrorist content online effectively? Should these be taken by larger companies, public authorities or both?

Les carences des petites entreprises en matière de modération des contenus illicites procèdent souvent de leurs ressources humaines limitées et de leurs ressources insuffisantes pour mettre en place les outils de détection appropriés. La **mutualisation des moyens entre petits et grands opérateurs** doit donc être encouragée.

Une incitation à la mise en place de systèmes d'alerte et de détection automatisée au sein des entreprises afin de faciliter le traitement humain pourrait être envisagée, l'Etat pourrait inciter, notamment via certaines aides, les entreprises concernées.

[4] See point 40 of the Recommendation.

7. Do you think that the voluntary approach is **effective** and flexible enough to ensure that companies continue their efforts in the **long term**? Please indicate with which statement you would agree with:

	Yes
	No, it should be reinforced as presented above to obtain sufficient guarantees
X	No, it should be reinforced via legislation

Nous ne pouvons faire reposer entièrement sur le dialogue établi avec une partie des entreprises l'efficacité de long terme de la lutte menée contre les contenus terroristes en ligne. L'UE doit donc poser un cadre juridique clair, ne serait-ce que pour que les entreprises aient une compréhension exhaustive de leurs responsabilités.

III. Legislative options

1. Why would you consider **legislation necessary at this time**? What would be the concrete benefits? What **risks** could legislation entail?

1/ Les travaux réalisés en France dans le cadre du GCP qui réunit les services du MI, de la Justice et les grands opérateurs américains de l'Internet (Facebook, Google, Twitter, Apple et Microsoft) et le dialogue engagé au plan européen dans le cadre du Forum de L'internet ont permis de réelles avancées (telle que la récente collaboration de Telégram).

La dernière réunion de l'EU Internet Forum du 22 mai a été l'occasion par ailleurs de souligner l'effort de transparence incontestable de certaines entreprises sur les métriques : 13 d'entre elles (sur toutefois 33 interrogées) ont présenté des données relativement fournies voire complètes, pour le premier trimestre 2018, conformément à la matrice que nous avons établie avec Europol pour arriver à la nécessaire corroboration et réconciliation des chiffres avec les Etats membres de l'UE.

2/ Malgré l'amélioration générale que notre dialogue nous a permis d'enregistrer, plusieurs de nos attentes restent insatisfaites :

Un texte législatif européen permettrait d'harmoniser les obligations et assurer une égalité de traitement entre tous les opérateurs qui proposent un service sur le territoire de l'Union (notamment à la faveur des opérateurs européens, lesquels sont aujourd'hui beaucoup plus réactifs).

3/ Dès lors, nous ne pouvons faire reposer entièrement sur le dialogue établi avec une partie des entreprises l'efficacité de long terme de la lutte que nous menons contre les contenus terroristes en ligne. Nous devons poser un cadre juridique clair, ne serait-ce que pour que les entreprises aient une compréhension exhaustive de leurs responsabilités.

Face à l'urgence, un projet de législation au niveau UE doit être proposé : il doit viser notamment à imposer aux entreprises, la détection proactive de contenus terroristes et le retrait rapide de tels contenus. Nous savons en effet qu'au-delà d'une heure, l'essentiel de la dissémination d'un contenu est fait. Il est aussi nécessaire d'imposer aux entreprises, la désignation d'un point de contact, des obligations de transparence sur les méthodes de modération et les moyens affectés à cette mission, sur le modèle de la récente loi allemande sur les contenus illicites; d'imposer la conservation des contenus retirés, afin de faciliter le travail d'enquête des services de police et de justice ; de favoriser l'amélioration des moyens d'identification des auteurs.

Ce texte doit être un premier pas, qui prépare les évolutions législatives dont nous avons besoin pour lutter efficacement contre les contenus illicites dans leur ensemble, et notamment les contenus haineux, qu'ils soient racistes, antisémites, anti-islamiques ou homophobes.

Sur ce point en effet, la politique de retrait des contenus des opérateurs (hors UE) reste peu lisible. [redacted]

2. What should be the **material scope of legislation** (i.e. how should terrorist content be defined)? Do you consider that covering material inciting to commit terrorist acts (Article 21/Article 5 of the Terrorism Directive[5]) is sufficient or should the dissemination of material pursuing other terrorist purposes be included as well?

Material the dissemination of which pursues the following objectives should be included in legislative measures:

	Recruitment for terrorism
	Providing training for terrorism
	Terrorist financing
	Other, please elaborate: voir ci-dessous

To what extent should material produced by UN/EU designated terrorist organisations be included?

La plateforme PHAROS n'est confrontée que de manière très marginale à des problématiques de qualification des contenus de propagande terroriste. Compte-tenu d'une jurisprudence extensive, les incriminations de l'apologie du terrorisme et de la provocation aux actes terroristes permettent de prendre les mesures administratives et judiciaires qui s'imposent pour l'ensemble des contenus de propagande terroriste signalés.

Un «contenu à caractère terroriste» pourrait être défini comme suit :

a. toute information dont la diffusion constitue une infraction au sens de la directive (UE) 2017/541 ou une infraction terroriste au sens de la législation de l'État membre concerné, ce qui englobe la diffusion d'informations de ce type émanant de groupes ou d'entités terroristes figurant sur les listes établies par l'Union ou les Nations unies, ou attribuables auxdits groupes ou entités

b. toute information dont la diffusion facilite ou incite à la commission d'infractions terroristes, au sens de la directive (UE) 2017/541

[5] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541

3. Which **measures** (based in particular on the elements mentioned in the Inception Impact Assessment) do you consider as **necessary elements of legislation** to be impactful? Please indicate the need from a scale from 1 (unnecessary) to 5 (very necessary)

5	Definition of terrorist content (*see question above*) Infraction au sens de la directive (UE) 2017/541.
5	Requirements regarding the companies' terms of service (Cf. Question III 1)
5	General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)
5	Specific requirements in terms of action upon referral (including time limit of one hour) (Cf. Question III 1)
5	More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)
5	Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms
5	Sanctions in case of non-compliance (volonté présidentielle plusieurs fois réaffirmée)
5	Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material
4	Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)
4	Requirement to Member States to increase referral capabilities, quality criteria for referrals and for referral entities in Member States to provide relevant support to companies in case of doubt about qualification as terrorist content (e.g. through points of contact)
5	Nomination of point of contact within Companies
5	Reporting obligations for companies[6]
4	Transparency requirements for companies vis a vis their users[7]
4	Compulsory safeguards, such as the ones in the general chapter of the Recommendation
5	The establishment of an external audit/monitoring mechanism for assessing compliance of companies.

Do you consider that minimum requirements could usefully be complemented by self-regulatory measures? And if so, which ones?

Question à préciser

4. What **other additional measures** could be developed within legislation?

---

6 See point 41 of the Recommendation.

7 See points 16 and 17 of the Recommendation.

Voir pj sur la proposition d'une directive européenne

Et Voir les réponses supra relatives à l'obtention de la preuve numérique

5. What should be the **personal scope of the legislation**? Only hosting service providers within the meaning of the Directive on electronic commerce or other service providers?

Le retrait des contenus illicites dépend des fournisseurs de services d'hébergement. La définition juridique de ces opérateurs doit être adaptée pour englober **l'ensemble des entreprises concernées**, compte-tenu de l'évolution des techniques et des pratiques.

Les hébergeurs ne se contentent plus de stocker les données mais sélectionnent, référencent, classent, mettent en avant et recommandent (grâce au profilage de leurs utilisateurs et à des algorithmes prédictifs ou de suggestion) les services et les contenus, voire les monétisent.

Le régime de l'hébergeur, pensé délibérément de façon étroite pour n'embrasser que certaines opérations techniques qui permettent d'améliorer la circulation des données sur le Web, se trouve ainsi aujourd'hui appliqué à des opérateurs (réseaux sociaux y compris) dont les activités dépassent largement le simple stockage ou le transit d'informations mais consistent à donner accès au public à des contenus diversifiés.

Le rôle de certains hébergeurs ne peut plus être aujourd'hui assimilé à celui d'un hébergeur classique. La distinction binaire entre l'hébergeur passif et l'éditeur actif n'est plus en mesure de rendre compte des réalités de l'écosystème numérique et du rôle structurant joué par certaines plateformes. Le droit doit évoluer pour prendre en considération cette nouvelle donne.

6. Do you think **smaller companies** should be covered by all obligations or should they be exempted from some of the obligations (e.g. proactive measures) but obliged by others (e.g. time-limits after referral)? Which companies could be partially exempted and from which obligations?

Les petites entreprises doivent être exemptées d'une partie des obligations (par exemple l'obligation d'avoir un représentant dans chaque EM).

Pour le reste de la réponse, voir proposition de texte UE.

7. How do you see the **impact on fundamental rights** of the above-mentioned measures and which safeguards would be necessary to avoid undue interference with fundamental rights?

Voir proposition de texte UE