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	Domestic legislation that regulates Judicial Cooperation Requests for terrorist cases, including Mutual Legal Assistance Requests and for the sharing of Digital Evidence. i. Law 144/1999, of 31 of August (International cooperation in criminal matters). ii. Law 109/2009, of 15 of September (Law on cybercrime) iii. Law 32/2008, of 17 of July (Law on electronic communications data preservation). iv. Law 67/1998, of 26 of October (Law on personal data protection). v. Law 36/2003, of 22 of August (Status and competence of the national member of EUROJUST). vi. Law 37/2008, of 06 of August (Legal and functional status of the Judiciary Police). vii. Decree-Law 42/2009, of 12 of February (Law establishing the Judiciary Police units competencies) viii. Law 52/2003, of 22 of August (Counter-Terrorism Law)
Transparency rules	
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)?

The main institutions involved in the fight against terrorism are the following: The Public Prosecutors are responsible for the criminal investigation and prosecution of all crimes. However, the criminal investigation could be delegated to the Judiciary Police (Polícia Judiciária) which performs its tasks under the direction and supervision of the Public Prosecutor in charge of the criminal inquiry. According to the Status of the Public Prosecution Service, the Central Department for Criminal Investigation and Prosecution (Departamento Central de Investigação e Ação Penal - DCIAP) is the responsible body to direct the inquiry and carry out the prosecution of terrorism offences, whenever the criminal activity occurs in

[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

regions pertaining to different judicial districts. The DCIAP is also competent when the Attorney General considers that a centralized direction of the investigation is required, taking into consideration the seriousness of the crime, the particular complexity or the extent of the criminal activity throughout the national territory or extraterritorially. The Judiciary Police which is the law enforcement organ competent for the investigation of terrorism offences in Portugal, holds within its structure, a special unit devoted to the fight against terrorism — the Counter-Terrorism National Unit (Unidade Nacional Contra Terrorismo - UNCT).
Concerning counter online radicalization and recruitment to terrorism, the Counter-Terrorism National Unit (Unidade Nacional Contra Terrorismo - UNCT) is the national contact point of EU IRU being responsible for the referral of violent extremist content located in Portugal.
On a general perspective, Decree-Law 7/2004, of 7 January (which transposed e-Commerce Directive in Portugal) stipulates that competent authorities, within their given sectors (or ANACOM, as central supervisory authority, only if and where no sectoral competent authority exists) have the powers:
a) to order the blockage of access and/or removal of webpages, subject to and in accordance with any specific legal regime providing for such power; and
b) to provisionally solve (within 48 hours) conflicts between any party interested in the removal/maintenance of a given content and a the relevant hosting or content aggregation service provider.
Concerning the co-operation with the private sector, ANACOM, both in the context of the legal framework of the Electronic Communications Law and in accordance with its Statute, has among its roles the promotion of technical standardization in the electronic communications sector and related areas, in particular in collaboration with other organizations.
In this context, ANACOM promotes the debate on the standardization of work in the area of security of information systems, in specific in what regards electronic communications by involving sector representatives.
ISPs, even if they are not under a legal obligation, are members of CERT.PT. The purpose of CERT.PT is that of improving efficiency in regard to the reaction to cybersecurity incidents in Portugal, by means of facilitating the share of relevant information, coordinating mitigation and resolution actions within the involved several entities, and the remaining national and international authorities.

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

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?

EU IRU works in increased reporting on referrals. Europol supports a network of national IRUs to promote co-operation, co-ordination and the exchange of knowledge and best practices on referral capabilities.

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?

There is a high risk of interference. One way could be having coordination of investigations through EUROPOL.

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?

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?

Yes, there was some progress but it does not guarantee all the OSP efforts effectiveness.

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)?

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)
	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].
	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)
2	More detailed requirements on transparency and reporting
	More detailed requirements to companies on safeguards against over-removal
1	Establishment of an external audit/monitoring mechanism
4	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.
3	Additional support (e.g. by Europol) to referral capacities in Member States

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

[4] See point 40 of the Recommendation.

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

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?

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

II. Legislative options

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

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:

[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

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

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)

	Definition of terrorist content (*see question above*)
	Requirements regarding the companies' terms of service
	General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)
	Specific requirements in terms of action upon referral (including time limit of one hour)
	More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)
	Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms
	Sanctions in case of non-compliance
	Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material
	Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)
	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)
	Nomination of point of contact within Companies
	Reporting obligations for companies[6]
	Transparency requirements for companies vis a vis their users[7]
	Compulsory safeguards, such as the ones in the general chapter of the Recommendation
	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?

[6] See point 41 of the Recommendation.
[7] See points 16 and 17 of the Recommendation.

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

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?

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?

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?