034767/EU XXVI. GP
Eingelangt am 14/09/18

Council of the European Union

**Brussels, 14 September 2018**
**(OR. en)**

**12129/18**
**ADD 2**

**Interinstitutional File:**
**2018/0331(COD)**

**CT 144**
**ENFOPOL 450**
**COTER 114**
**JAI 881**
**CYBER 193**
**TELECOM 288**
**FREMP 142**
**AUDIO 64**
**DROIPEN 127**
**COHOM 107**
**CODEC 1468**

**COVER NOTE**

| | |
|---|---|
| From: | Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director |
| date of receipt: | 12 September 2018 |
| To: | Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union |
| No. Cion doc.: | SWD(2018) 408 final |
| Subject: | COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online |

Delegations will find attached document SWD(2018) 408 final.

Encl.: SWD(2018) 408 final



www.parlament.gv.at

EUROPEAN
COMMISSION

Brussels, 12.9.2018
SWD(2018) 408 final

# COMMISSION STAFF WORKING DOCUMENT

# IMPACT ASSESSMENT

***Accompanying the document***

**Proposal for a Regulation of the European Parliament and of the Council**

**on preventing the dissemination of terrorist content online**

{COM(2018) 640 final} - {SEC(2018) 397 final} - {SWD(2018) 409 final}



www.parlament.gv.at

## Table of contents





www.parlament.gv.at

# 1. INTRODUCTION

## 1.1. Political and legal context

The availability and proliferation of illegal content online represents a very important public policy and security concern in the EU. This impact assessment report focuses in particular on the availability and spread of terrorist content on online hosting services, and analyses a series of legislative options.

The Commission has been working on the issues of terrorist content online, but also on other types of illegal activities online, such as illegal hate speech, child sexual abuse material (CSAM), and illegal commercial practices such as infringements of intellectual property rights, selling of illicit drugs, counterfeits or other illicit goods create significant harm in society and reduce trust in the digital economy.

Illegal content is shared online in particular through online services that allow upload of third party content, also known as hosting service providers. At EU level, the general legal framework for illegal content removal by hosting service providers is provided by the E-Commerce Directive1, which balances the need for effective action for illegal content removal, safeguards against over-removal of legal content, and promotes growth and innovation in the Digital Single Market. Building on this general legal framework, the Commission has reinforced and strengthened the fight against illegal content online with a series of regulatory and non-regulatory initiatives. The regulatory initiatives include the Directives combatting the child sexual abuse material 2011/93/EU, combatting terrorism (EU) 2017/541, as well as the recently agreed revision of the Directive on audio-visual media services 2016/0151 (COD), and the proposal for a Directive on Copyright 2016/0280 (COD). In addition, the Commission's Recommendation on measures to effectively tackle illegal content online C(2018)1177, and the Communication on tackling illegal content online COM 2017/555 cover all types of illegal content and offer guidance to hosting service providers and authorities. These initiatives have been complemented by a series of voluntary initiatives, such as the Code of Conduct on combatting Hate Speech adopted in May 2016, the EU Internet Forum on terrorist content online launched in December 2015, as well as the June 2016 Memorandum of Understanding on counterfeit goods sold online.

Despite these initiatives, there remains a particular concern about the availability of terrorist material online. In 2017, there were a total of 205 foiled, failed and completed terrorist attacks in the EU, which killed over 68 and injured over 800[2]. The continued high level of terrorist threat in the EU is accompanied by continued concern about the role of the internet in aiding terrorist organisations to pursue and fulfil their objectives to radicalise and to recruit, to facilitate and direct terrorist activity.

In June 2018, the European Council called upon the Commission *'to present a legislative proposal to improve the detection and removal of content that incites hatred and to commit terrorist acts'*. This followed previous calls from the European Council of 22-23 June 2017 for industry to '*develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts. This should be complemented by the relevant legislative measures at EU level, if*

1 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

2 Europol's Terrorism Situation and Trend Report 2018



www.parlament.gv.at

*necessary'*. Similarly, the European Parliament, in its resolution on Online Platforms of June 2017, urged the platforms concerned "*to strengthen measures to tackle illegal and harmful content*", and called on the Commission to present proposals to address these issues. These calls were echoed by statements issued by the leaders of the G7 and G20 in 2017 in the shared fight against terrorism.

Tackling terrorist content online is part of a broader comprehensive approach to counter terrorism, which includes the criminalisation of terrorist offences and prosecution of perpetrators, as foreseen under the Terrorism Directive (EU) 2017/541. Whilst ideally perpetrators will always be brought to justice, some of the material is produced in war zones and ungoverned territories, outside of the EU, making it difficult for EU law enforcement to successfully investigate and prosecute. Whilst the prosecution of terrorist perpetrators remains a priority, of equal importance is to reduce the accessibility to online terrorist content online so as to protect online users from such harmful content and to make it harder for terrorists to operate online.

Therefore the main focus of this Impact Assessment is to assess problems related to terrorist content online, its impact on the Digital Single Market and options to further reduce its availability. The impact of these options on, as well as the complementarity to, criminal investigation will be part of the assessment.

## 2. PROBLEM STATEMENT

### 2.1. Scope and further context

Internet access continues to expand across the globe, while at the same time it becomes ever easier and cheaper to create and disseminate content online, allowing users to connect and share information with billions of individuals across the globe. Almost 70% of Europeans are regular users3 of social media; a similar share watch videos or live-streaming, or listen to music online regularly, 47% use file storage or sharing services regularly, 51% engage on review and rating platforms and a similar share read blogs, comment on articles or news websites.

However, the ability to reach such a large audience with minimum cost also attracts individuals who want to use the Internet for illegal purposes. The presence of illegal content is a concern for users and citizens at large, public authorities as well as online hosting services providers. These services now store unprecedented amounts of third-party content and information. A rich and diverse ecosystem of such hosting services has emerged across the globe, consisting of some very large service providers, but also many small and specialised ones. **Services in scope** of this analysis cover a range of business models and a mix of hosting services such as content storage and distribution services (e.g. web hosting, file sharing, online media sharing), networking, collaborative production and matchmaking (e.g. social networks, marketplaces, online games), and selection and referencing services (e.g. online search tools, rating platforms)[4].

Each company is free to conduct its business under their preferred business model, and to set out and apply its terms of service to define the content it is willing to host. Hosting service providers have a complex set of incentives relating to their own policies towards illegal content online, depending on their size, profitability, reputation, and business model, which includes incentives to maintain trust in its services (in particular by avoiding the proliferation of illegal content on its services). The scale

3 61% use social media at least a few times a week; 7% use it several times a month, cf Flash Eurobarometer 469 (2018)

4 J. VAN HOBOKEN et al., *Hosting Intermediary Services and Illegal Content Online* (forthcoming), pp 5-6 The study analysed the business models offered by hosting services from an economic and legal perspective.



www.parlament.gv.at

and speed necessary for effective content moderation has spurred companies' action to protect their users as well as their own reputation, taking into account that they are often best placed to swiftly act against any illegal or harmful content that they host. Service providers may also have incentives not to take any action against such content being disseminated on its platforms taking into account their users preferences.

The dissemination of illegal content online continues to be of strong and urgent societal and political concern. To tackle this issue, the relevant legal framework includes the general provisions set out in the E-Commerce Directive, and targeted instruments, some of which have been recently adopted or under negotiations, and which should produce their effects in the near future. This includes the Directive on Combatting Terrorism, proposed measures in the context of the revision of the Audiovisual Media Services Directive (AVMSD), and the proposal for a Directive on Copyright in the Digital Single Market. Other relevant legal acts include the Directive against Child Sexual Abuse, or the Directive on the Enforcement of Intellectual Property Rights.

The Commission's 2017 Communication and 2018 Recommendation have started to bear fruit, but have not yet produced their full effect across all types of illegal content. Besides these recent non-binding initiatives, the Commission continues to support and to monitor targeted voluntary cooperation with industry:

On **illegal hate speech,** reporting on the implementation of the Code of Conduct shows that the voluntary collaboration can yield very positive results in a relatively short time. A key indicator is the progress made to achieve the takedown of 70% of the content reported as hate speech. Considering the careful balance which needs to be struck in the takedown of illegal hate speech and the high risks of misidentification on lawful speech as illegal, this indicator shows good progress since the beginning of the cooperation. The strategic priority in this area is to extend the cooperation to a broader number of hosting services, expected to further improve the situation.

With regards to **counterfeit products** the recent guidelines5 released by the Commission should give further clarity to hosting services and improve the results of the specific measures. In addition, the Memorandum of Understanding is bringing results which show a positive evolution and are expected to further improve. Other voluntary actions are tackling the problem from different angles, most recently through a Memorandum of Understanding on online advertising, signed on the 25th June and aiming at further incentivising website owners to take vigilant action against the sale of counterfeit products on their platforms.

On **CSAM**, the work of the WePROTECT Global Alliance to end child sexual exploitation online, and the long-standing EU support to the INHOPE network of hotlines on child sexual abuse content continue to make progress. The analysis of the current situation, including the effects of the implementation of Directive 2011/93/EU, is ongoing and is expected to be finalised by the end of 2020. Therefore, legislating at this point in the area of child sexual abuse material would be premature as the necessary evidence is still being collected.

On **other types of illegal content,** legal proposals (e.g. Copyright Directive, New Deal for Consumers) or emerging cooperation (e.g. Consumer Protection Joint Action) cover further action and are expected to yield positive results.

Similarly, in the case of **terrorist content online**, ongoing efforts under the EU Internet Forum are bringing positive results. However, while the Commission continues its efforts and monitors closely

5 https://ec.europa.eu/docsroom/documents/26582



www.parlament.gv.at

the effectiveness of measures concerning other types of illegal content, there is a particular sense of urgency for effective policy intervention against terrorist content spreading online, as highlighted by the Commission in its Recommendation and as called upon by the European Council. The changes in operations of terrorist organisations lead to the unpredictable and unprecedented use of hosting services for disseminating terrorist propaganda. Content is often hosted by various small service providers, then shared through mainstream social media. The voluntary efforts and collaboration are bound by their natural limitations of only gathering a relatively small number of hosting service providers, and fail to spread good practice and gather sufficient impact and transparency from the hosting services most affected at any given time by the spread of terrorist content. Furthermore, speed is of the essence to remove terrorist content, therefore further efforts are needed to detect content as fast as possible, as well as removing flagged content quickly to avoid further dissemination across platforms and subsequent harm. In addition, the fragmentation of procedural rules across Member States limits the effectiveness and efficiency in the cooperation between authorities and hosting service providers.

This impact assessment analyses the problems arising from the use of hosting service providers for spreading terrorist content online, and proposes and analyses the potential impacts of further legislative measures.

**Stakeholders' views on the scope of a possible EU intervention**

Stakeholders' views have changed over time, in light of the emerging sector-specific legal initiatives and results of the voluntary cooperation. In past consultations starting with 2010, 2012, and even 2016, the majority of hosting service providers was pointing to the need for further legal certainty and harmonisation in respect to the notice-and-action procedures.

In the 2018-run consultations, service providers were rather supporting continuing targeted voluntary actions or very targeted, content-specific interventions, focusing on terrorist content. This follows the new steps taken with the adoption of soft instruments by the Commission – i.e. the Communication, and the Recommendation on measures to tackle illegal content online.

An important number of Member States, especially the majority of those most directly affected by terrorism, have called for legislation specifically in the area of terrorism. The European Council in its conclusions in June 2018 has called upon the Commission to take legal initiative to tackle the dissemination of terrorist content online.

## 2.2. Problem tree

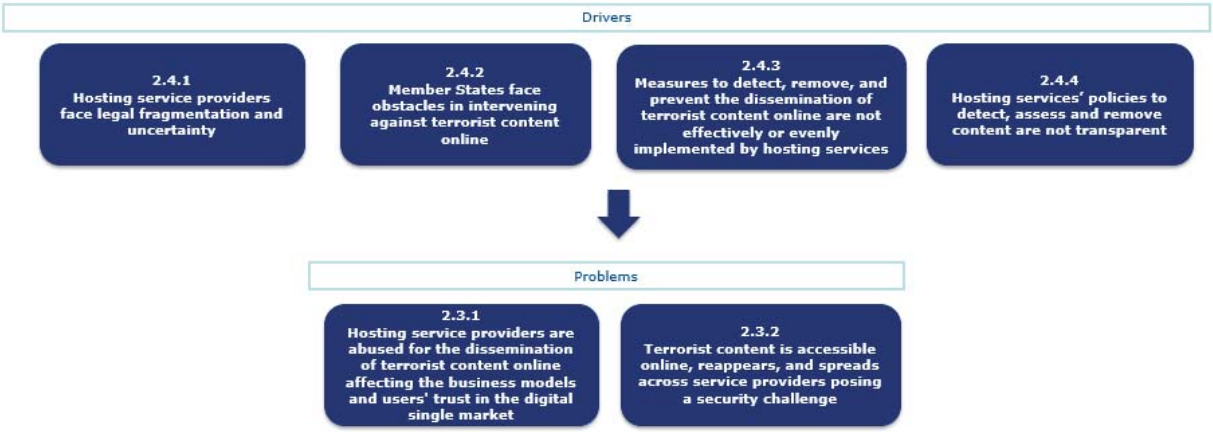



*Figure 1 Problem tree*



www.parlament.gv.at

## 2.3. What are the problems?

The dissemination of terrorist content online is an overall problem which is affecting private and public interests, hampering trust, innovation and growth in the Digital Single Market, and affecting public security in the EU.

### *2.3.1. Hosting service providers are abused for the dissemination of terrorist content online affecting the business models and users' trust in the digital single market*

While the Internet plays a crucial role enabling instant access to information, content and knowledge across borders, online hosting services are in certain cases abused by third parties to carry out illegal activities online, notably the dissemination of material related to terrorism.

Hosting illegal content creates important reputational damage on **companies;** it can affect a company's **business model,** affecting relations with users consuming or providing content, or advertisers, and other interconnected services. Social networks and media sharing platforms, whose business model is often based on advertising, have faced intense public criticism when terrorist or other illegal content was reported on their networks. This has in some cases triggered direct revenue loss, following a major backlash from certain advertisers, and led to user distrust6. Similar incidents were also reported by other business models such as web hosting services.

Estimates point to a basis of over **10.500 hosting service providers established in Europe**, and almost 20 000 HSPs established both in Europe and in the US and Canada. **Over 90% of European hosting services are SMEs,** amounting to roughly 9700 companies7, over 45% of which are micro-enterprises, and 40% medium-sized businesses8. SMEs offering hosting services are particularly vulnerable to exploitation for illegal activities, not least since they tend to have limited capacity to deploy state-of-the-art content moderation tools or specialized staff. Whilst the percentage of referrals sent to micro, small and unregistered companies only amounted to 7% in 2015 (when the EU IRU was first set up), they amount to 68% today.

Europol reports that over **150 companies** were identified as hosting terrorist content, a large part of them being established outside of Europe and offering their services across the Single Market. Data on location of users accessing the services identifies only two likely to operate in a single Member State.9

**More than half of these companies offer file storage and sharing services**. Most of these are SMEs, and reach a very limited audience (median of 20 000 views per month10, with a first quartile including below 1000 views). **Around 20% are online media sharing services (**including audio-visual media sharing platforms), half of which have a limited audience in Europe (average number of monthly views below 250.000), the rest reaching an audience of over 1 million users per month, and the large multinational companies reaching hundreds of million views. **Just under 10% offer web-hosting services**. **Just under 10% are social networking and discussion forums**, half of which

6 E.g. https://www.thetimes.co.uk/article/google-faces-questions-over-videos-on-youtube-3km257v8d

7 Estimates based on data available in the Dealroom database, https://dealroom.co/

8 Percentages based mostly on number of employees criterion; turnover approximated for most companies.

9 Cross-border presence inferred from https://www.similarweb.com/ traffic data monitored for a sample of 8 Member States from January 2017 to May 2018. The evolution of the numbers of unique views of the webpages is in this case a reliable proxy for the geography of users viewing content uploaded on the service, and, to certain extent, for the users uploading content. This varies depending the type of hosting service provided.

10 Number of views computed on the basis of the SimilarWeb database. These are rough proxies of scale for the user base of the hosting services, generally fit to draw a comparison across services, but cannot be used as such as indications of thresholds



www.parlament.gv.at

have less than 150 000 views, with the major social media platforms as outliers with a very large user base. **A very small number are online market places, collaborative production services, or selection and referencing services.**

**Consumers** using hosting services also incur the negative consequences. 61% of respondents to the dedicated Eurobarometer claim to have seen online some type of illegal content, the vast majority point to some sort of scams, frauds or illegal commercial practices. 6% of respondents claimed to have seen terrorist content online, reported exposure is however 11% for young people aged 15-24.

**Stakeholders' views**

In the various consultations carried out in the context of this impact assessment, hosting service providers underlined the challenge raised by the **volume** of illegal online content and acknowledged their **negative to very negative impact on their users and on their reputation**. This was in particular confirmed by companies reporting, in the context of the EU Internet Forum, on the presence of terrorist content on their service, affecting relations with users, content creators, advertisers, but also payment processors.

On the other hand, 65% of the respondents to a Eurobarometer on illegal content carried out in June 2018 did not consider the Internet to be safe for its users. In the public consultation, on the other hand, 75% of the respondents considered the internet to be safe. This divergence could be explained by the fact that the phone-run Eurobarometer collected the views of a representative, randomly built sample of 33 000 EU citizens, both users and non-users of online hosting services, whereas the internet based public consultation received 8749 replies from individuals, self-reported frequent Internet users, and self-selected in the sample by voluntarily replying to the consultation.

### *2.3.2. Terrorist content is accessible online, reappears, and spreads across service providers posing a security challenge*

Given its illegal nature but also the lack of systematic reporting on terrorist content identified online, comprehensive and fully reliable numbers of illegal content available online cannot be established. However, reports on the amount of content removed by certain companies, the number of pieces of content referred by public authorities or figures produced by research can give an indication of the size of the problem11.

For example, Europol's IRU has made over 50,000 decisions for referrals to service providers about terrorist content in their platforms since July 201512 and the UK's Internet Referral Unit (CTIRU) identified 300,000 pieces of terrorist content between 2010 and 201813. However, for those companies that are taking proactive measures to identify terrorist content themselves, in general, referrals only account for a small proportion of the total content removed. For example, Twitter has suspended over 1.2 million accounts for violations of their Terms of Service related to the promotion of terrorism between August 2015 and December 201714 and Facebook took action on 1.9 million pieces of Daesh and al-Qaeda content in the first quarter of 201815.

The terrorist group Daesh, which since its beginning has put in place an aggressive communication strategy, has been producing an average of ~1200 new propaganda items every month in 2015-2017, according to research surveys16. This material spreads online across various service providers

11 Estimates of actual access to illegal content are difficult to assess, and are generally based on reported data from hosting service providers, and, consequently, refer to content already identified as allegedly illegal. With the methodological caveat in mind, the estimates do give a valuable indication on the effectiveness of measures in place

12 TE-SAT 2018, https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018

13https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

14 https://blog.twitter.com/official/en_us/topics/company/2018/twitter-transparency-report-12.html

15 https://newsroom.fb.com/news/2018/04/keeping-terrorists-off-facebook/

16 VOX-Pol Network of Excellence, http://www.voxpol.eu/



www.parlament.gv.at

through link-sharing and reposting, as illustrated in Figure 2. While in January 2018 the number of new items of official Daesh propaganda in January 2018 had gone down to 700, it also represents a recent increase from 300 items in December 2017.

According to Europol17, by 2017 over 150 social media platforms were identified as being abused by terrorists for propaganda dissemination. Other analyses point to a number of 400 online platforms being misused by Daesh supporters for spreading terrorist material in 2017, of which 145 service providers were identified for the first time in the second half of the year as being abused18. According to Europol, whilst industry and law enforcement action have resulted in a reduction of the terrorist abuse of larger mainstream providers, similar progress has yet to be made with start-up social media and companies with limited resources.

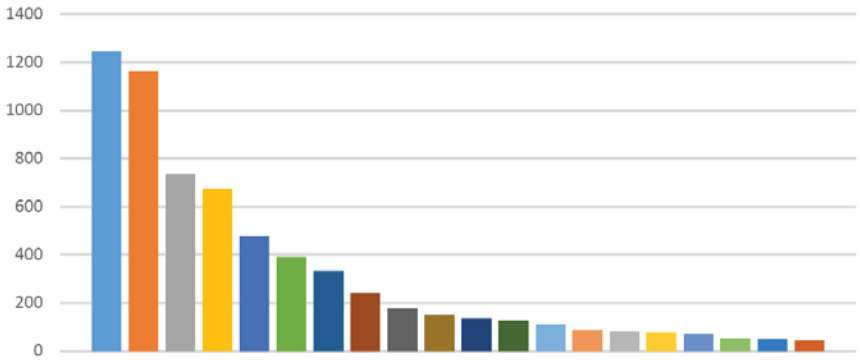



*Figure 2*

*Shares of links to Daesh propaganda hosted on the top twenty service providers in Q1 2018. While the four most affected providers have reduced the amount of Daesh links they host by approximately 80% since Q2 2017, the total amount hosted in the other 16 most affected platforms has barely decreased in absolute numbers. These 16 companies hosted around 10% of Daesh links out of the 20 most affected companies in Q1, a share that increased to around half in Q4 2017 and one third in Q1 2018* [19]

Another important indicator is how quickly terrorist content spreads across providers. Terrorist content is considered most harmful in the first hours of its appearance because of the speed at which it is disseminated and therefore multiplied. Research20 has found that one third of all links to Daesh propaganda is disseminated within 1 hour of release, and three quarters of all links are shared within four hours of release21.

In summary, terrorist content is not always detected at the point of uploading, is not sufficiently quickly removed when flagged to companies, and continues to move easily from one platform to another, allowing terrorists to operate online to intimidate, to groom and recruit, to facilitate and direct terrorist activity, and to glorify in their atrocities.

**Stakeholders' views:**

During consultations with Member States two Member States reported an increase or substantial increase of the amount of terrorist content online, four indicated that the situation remained the same and twelve that terrorist content online has decreased. Decrease in volume was mostly attributed to losses incurred by Daesh and to the voluntary efforts undertaken in particular by the large internet companies as well as Internet Referral Units. However, Member States underlined the

17 TE-SAT 2018 https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report
18 https://www.gov.uk/government/news/new-technology-revealed-to-help-fight-terrorist-content-online
19 RICU Analysis, June 2018
20 Announced in a press release in February 2018 https://www.gov.uk/government/news/new-technology-revealed-to-help-fight-terrorist-content-online
21 RICU Analysis, June 2018



www.parlament.gv.at

dispersal of terrorist content across a greater number of smaller service providers as an emerging trend posing a persistent security challenge.

## 2.4. What are the problem drivers?

### *2.4.1. Hosting service providers face legal fragmentation and uncertainty*

The E-Commerce Directive establishes in its Article 3 the country of origin principle, following which providers of information society services have to comply with the law of the Member State where they are established. This principle, pursuant to which Member States are not allowed to restrict the provision of services from another Member State, represents the cornerstone of the Digital Single Market. Restrictive measures against a given information society service provider established in a different Member State can only be allowed if they are necessary and proportionate to protect objectives of public policy, public security, public health or protection of consumers.

The EU presents a patchy legal framework as regards the possibility for national competent authorities and courts to request the takedown of illegal terrorist content, or the blocking of websites publishing such content. In the majority of the cases, the order has to stem from a jurisdictional body, but some legislations allow for an administrative order – subject to court appeal. These laws cohabit with non-regulatory practices based on the voluntary cooperation by online services providers, based on the implementation of their own terms of service.

This is also reflected in the transposition of the Directive on Combatting Terrorism. Article 21 calls on Member States to put in place measures to ensure swift removal of content inciting to the commission of terrorist acts. Fifteen Member States have informed the Commission that they have already transposed it. The information about transposition measures refers to existing or amended legislation allowing a prosecutor or a court to order companies the removal of content or the blocking of content or a website. In some cases, there are time limits of 24 hour or 48 hours for companies to take action. In most cases, however, these powers can only be exercised within a criminal procedure.

Member States also have in place measures in-line with the transposition of the E-Commerce Directive's Article 14 (3) for establishing procedures governing the removal or disabling of access to information. Annex 7 presents in detail the different provisions in Member States' law, governing procedures for notification by national authorities related to terrorist content in particular22. These measures have a different scope in terms of offences covered, time limits for removal and consequence of non-compliance. In some cases notice-and-action procedures are limited to manifestly illegal content (Austria, France, Portugal), which includes in some instances terrorist content. Only recently, Germany included, under the NetzDG, some offences related to terrorist content such as disseminating propaganda material by unconstitutional organisations (including terrorist organisations), forming a terrorist organisation or encouragement the commission of a serious violent offence endangering the state. Another source of potential legal uncertainty is that, while terrorist offences are defined in the Terrorism Directive, there is at EU level no explicit definition of terrorist propaganda, contrary to provisions that exist under national law. 23 Some MS have legislation in place obliging hosting service providers to report to authorities when they identify illegal content (proactively or following a notice from a third party) and others are imposing the need for a legal representative to be established on their respective jurisdiction.

22 See Annex 7 for further information.
23 see Annex 7



www.parlament.gv.at

While so far limited to the field of copyright, national courts have followed different interpretations of the scope of duties of care ranging from a limited duty to take down (upon notice), to more extended duties to prevent also future infringements of the same kind under specific circumstances24.

At the same time, Member States are increasingly imposing transparency obligations on online hosting services, regardless of their place of establishment, with the purpose of increasing the public oversight on the way these intermediaries' implement their content policies and their reactions to notices25.

In addition, in a few Member States law enforcement authorities can issue removal orders and an important number of Member States have established mechanisms for law enforcement authorities to refer content for the voluntary removal of companies, allowing them to achieve faster removal outside a criminal procedure. Many Member States have established some sort of voluntary framework to facilitate cooperation with large HSPs.

The fragmentation across the administrative procedures entails significant costs for small and medium size hosting service providers offering their services cross-border. Companies face a legal complexity which makes it difficult and costly to comply with the different procedures and timeframes for removal of content and reporting obligations, and, importantly, fragmentation of definitions of what constitutes terrorist propaganda and the need to have a legal representative in the Member State's jurisdiction. There is a risk that legal fragmentation would further increase, and, on ground of national security, request exemptions from the country of origin principle. While this is in principle possible within EU law, the heavy costs of legal fragmentation could lead to either non-compliance or non-enforceability of the respective laws, or to insurmountable obstacles in particular to small European hosting service providers and blockages in the Digital Single Market.

**Stakeholders' views:**

Based on a specific questionnaire sent to companies on terrorist content, all responding companies acknowledged a serious concern posed by the risk of diverging legislation in different countries to address terrorist content online, and that smaller companies would suffer more from 28 different sets of rules, which could end up being used as a tool for competitive advantage by larger companies[26].

24 For instance, in France the Supreme Court (then followed by the Paris Court of Appeal) has consistently established, since 2012, that there is no obligation for providers of hosting services to prevent the reappearance of contents they have already taken down (often referred to as "*notice and stay down*" principle), except if they are formally notified by rights-owners again (French Supreme Court, 12 July 2012, no. 11-13.666, 11-15.165/11-15.188, 11-13.669). In Germany, in turn, Courts have consistently applied the Störerhaftung doctrine from civil law to intellectual property rights litigations to ensure that the hosting service provider prevents the commission of further infringements. In the UK, courts can impose dynamic injunctions in the field of intellectual property rights. The CJEU will decide on a case concerning prevention of reappearance of defamatory content (C-18/18, Glawischnig-Piesczek (Case pending)].

25 - The German Network Enforcement Act imposes on providers of social networks which receive more than 100 complaints per calendar year about unlawful content an obligation to produce very detailed half-yearly German-language reports on the handling of complaints about unlawful content on their platforms; the UK proposes plans for transparency reporting as part of the Digital Charter, which will provide data on the amount of harmful content being reported to platforms in the UK and information on how these reports are dealt with; the Council of Europe, in its Recommendation on the roles and responsibilities of internet intermediaries, which should inform Member States in their legislation-making decisions, recommends intermediaries to regularly publish transparency reports that provide clear (simple and machine-readable), easily accessible and meaningful information on all restrictions to the free and open flow of information and ideas and all requests for such restriction, as well as requests for data access and preservation.

26 Source: Terrorist content-related questionnaire for companies. See also Annex 3



www.parlament.gv.at

*2.4.2. Member States face obstacles in intervening against terrorist content online*

With regards to terrorist content online, the Commission has been engaging with over 20 companies, including many of the most affected and largest platforms, as part of the EU Internet Forum to support the implementation of an Action Plant to Combat Terrorist Content Online and the terrorism-specific measures foreseen under the Recommendation on illegal content. Whilst important progress has been achieved in terms of increased co-operation, improving responses to referrals, deployment of proactive measures and co-operation between the industry (including for example the Database of Hashes of content identified and removed by companies) as well as increased transparency, the Commission has struggled to establish contact with all companies affected by terrorist content. To better measure progress under the Recommendation, the Forum developed a set of indicators to enhance collective understanding of the level of effort being applied to reduce accessibility to terrorist content online. Of the 33 companies for whom the Commission had a point of contact, only 14 responded to the two requests for reporting on their efforts. A more detailed summary is set out below in Table 1

The difficulty in establishing contact with all the companies which are affected by terrorist content is due to a number of reasons. The Commission and indeed Europol and Member States do not have contact details for all the platforms affected. Whilst outreach efforts have been made with many, in some cases, it may be that the companies are completely unaware of EU initiatives and for some, it might be that they are aware but choose not to engage. This obstacle makes it difficult to process referrals or to have any meaningful discussion or co-operation with regards to terrorist content hosted on their sites.

Finally, another challenge arising from removal of terrorist content online is the risk of companies' removals interfering with investigations. All Member States responding to the terrorism-specific questionnaire highlighted this risk, since the online activities of a suspect can be crucial for law enforcement and the removal of his or her content can impair an investigation and reduce the chances of disrupting criminal activity and obtaining the necessary evidence for prosecution purposes. Furthermore, the content that terrorist groups disseminate online gives competent authorities key insights on the groups' messages, strategy and methods. Companies' removal of such content without retaining it or informing EU law enforcement or Europol, potentially risks hampering an essential source of intelligence and/or evidence for competent authorities to be able to effectively prosecute. Member States therefore consider it necessary to adopt measures to limit any interference with investigations and to ensure removed content is not lost but able to support operational and analytical requirements.

**Stakeholders' views:**

During stakeholders' consultation, Member States highlighted the progress achieved under the voluntary process. However, some also noted that regardless, the number of companies engaged remained limited. As exemplified by the reporting exercise under the Recommendation in which only half of the companies who were asked to provide data responded.



www.parlament.gv.at

### *2.4.3. Measures to detect, remove and prevent the dissemination of terrorist content are not effectively or evenly implemented by hosting services*

The Commission's Communication on tackling illegal content online27, as well as the subsequent Recommendation28 set out a number of measures governing the detection, removal and prevention of dissemination of illegal content online.

The Communication identifies different sources of information about the presence of illegal content and alleged illegal content on hosting services, from court orders or administrative decisions and notices from competent authorities (e.g. law enforcement bodies), specialised 'trusted flaggers', intellectual property rights holders to ordinary users. Hosting service providers have implemented specific procedures to various degrees for the different types of notices. Practices include trusted flaggers schemes for specific types of content, including, in some cases, fast removal of terrorist content referred by law enforcement. The Recommendation encourages hosting service providers to put in place notice and action procedures and to take specific proactive measures, including where appropriate automated detection tools (subject to the necessary safeguards). The Recommendation builds on and consolidates efforts under voluntary processes currently in place.

With respect to terrorism, initial insights into follow-up actions by hosting service providers show that the recommended measures are not being applied consistently by all. Those companies who have engaged under the EU Internet Forum have undertaken a number of actions and progress can visibly be seen. The table below summarises results, as reported by companies to the Commission.

*Table 1 Results reported by companies in the EU Internet Forum following the Commission's Recommendation*

| **Hosting services PARTICIPATING** | **Proactive takedown** (% of the total removed content, compared to content removed following notices) | **NUMBER OF referrals received** | **% REMOVALS (out of content notified** | **SPEED** |
|---|---|---|---|---|
| Reached out to 20 platforms, including. Facebook, Youtube, Microsoft, Twitter, Internet archive, Justpaste.it, Wordpress, snap, Soundcloud After Recommendation: Baaz, Dropbox, Mega, Userscloud, Telegram | Varies across companies: e.g. 44**% (Q2 2018) to 83% (Q4 2017)** reported by **one SME**; 99% by Facebook in Q1 2018 Database of hashes used by 13 companies | For EU IRU: Q4 2017**: 8,103 referrals** Q1 2018**: 5,708 referrals** | For EU IRU: Q4 2017: 89% Q1 2018: 61% (But between 96 and 100% for "big four": FB, YouTube, Microsoft and Twitter) | Proactive measures: 5 companies reported to remove content within 1h, out of which 3 companies could do it within 1 minute, using proactive measures. For referrals: majority of companies not removing within one hour; nevertheless some have jumped from 0% to 66% removals within one hour or 8% to 52%. |

With regards to referrals, Europol established an EU Internet Referral Unit (EU IRU) in 2015 to actively scan the internet for terrorist content and then refer it to the hosting service providers, accompanied by an assessment. This voluntary arrangement has resulted in over 50,000 decisions for referrals across over 80 services providers in more than 10 languages. The EU IRU works closely with its Member States' counterparts. The number of national IRUs has steadily risen to 6 and an additional number of Member States are active in this area but do not have IRUs as such. However, companies do not always respond in a sufficiently swift manner, despite efforts to reduce the life-span of such content online, and some companies do not respond at all to referrals. The majority of

27 COM(2017) 555 final https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms

28 Recommendation of 1 March 2018 on measures to effectively tackle illegal content online (C(2018) 1177 final).



www.parlament.gv.at

companies (whether large or small businesses) have not managed to remove content referred within one hour.

Whilst referrals are an important element of the response, it has become clear that referrals alone are not able to achieve the necessary impact with regards to volume and speed of removal. For example, it might be a matter of hours, or days, before IRUs identify a certain piece of content on a platform. By contrast, some companies using automated detection claim that content can be identified within a matter of minutes or less. Furthermore, where companies are using proactive measures, referrals only seem to amount to a very small percentage of the total amount of terrorist content removed. Nevertheless, the survival time of terrorist content online varies considerably across platforms, ranging from minutes to days, depending on whether proactive or reactive measures are employed.

Generally speaking, the longer the content is able to survive online, the more views it may receive, and the more harm it may cause. This is also linked to the fact that terrorist content is spread quickly and easily across platforms. Often terrorists or their supporters set up accounts in advance of publications in order to facilitate the swift dissemination of new terrorist propaganda items. Even where content is removed from one site, it can be uploaded onto other services, or even onto the same site from which it was previously removed. To address this challenge 13 companies are using a shared database of hashes including content identified as terrorist according to the companies' terms and conditions. The database is collectively used to prevent the re-uploading and dissemination of removed content across platforms. According to reporting by companies, the database includes over 80,000 distinct hashes of terrorist videos and images. Reporting suggests varying but increasing degrees of use as well as differences in the frequency of use by the participating companies. The feedback on the impact of the Database of Hashes in terms of content removed is still limited and is not systematic across platforms. Other tools to detect terrorist content, include the E-Glyph tool29, or Twitter's URL database.

No data is available for estimating costs of setting up, maintaining or using such a database. Costs can vary, from the use of simple (and not particularly reliable) hashing software, to 100 million EUR reported by one major video sharing platform for developing such advanced tools for filtering copyright protected materials.

Recently, two major online platforms have reported to be using machine-learning classifiers to flag content as possible terrorist or violent extremist material. Companies claim high levels of accuracy30 in flagging content for human review, but media reports have recently highlighted cases where the systems have misidentified content from conflict areas as being terrorist content.31 The UK Home Office has also reported the development of a tool by ASI Data Science32 to detect terrorist materials online.

For text detection, natural language processing is considered by and large immature for accurately identifying illegal hate speech or other violent speech33, and anecdotal reports point to

29 https://www.counterextremism.com/press/counter-extremism-project-unveils-technology-combat-online-extremism
30 No verifiable accuracy reports or independent checks available to date
31 http://www.wired.co.uk/article/chemical-weapons-in-syria-youtube-algorithm-delete-video
32 https://www.gov.uk/government/news/new-technology-revealed-to-help-fight-terrorist-content-online
33 A. SCHMIDT, M. WIEGAND, 'A survey of hate speech detection using natural language processing' in Proceedings of the Fifth International Workshop on natural Language Processing for Social Media, Spain, April 2017, http://www.aclweb.org/anthology/W/W17/W17-1101.pdf

misidentification and takedown of lawful speech[34] which show that automated detection of hateful content still needs to be combined with human verification.

While the cost of such tools varies depending on the type of content, they involve, besides highly skilled data science staff for development, access to an important volume of content to train the classifier, as well as substantial human verification to accompany and correct the training The Commission's Communication on tackling illegal content called for such automated tools to be deployed along with human verification before the takedown of content. This serves a double purpose: to train the classifiers, and to limit the erroneous identification by still immature tools, leading to removal of lawful content and limiting the possibility for users to express themselves freely.

Despite the efforts by some service providers, not all companies implement such tools, and the effectiveness or success rates of content taken down varies. Resource constraints (financial, technical and human review capabilities) may be of consideration, as well as proportionality of the efforts necessary, considering the risk, frequency and impact of illegal content companies might store at any given time. For some hosting service providers, the core value proposition of the service offered is the encrypted storage of data[35]; in these cases, the hosting service cannot access the content by design and, implicitly, does not run software to detect illegal content, but depends on external notices.

Micro, medium and small enterprises are particularly vulnerable facing illegal content which might be uploaded by their users. Discussions within the EU Internet Forum highlighted how small companies can be suddenly exploited for storing and disseminating terrorist propaganda. The EU Internet Forum has also offered a space for collaboration and support, allowing SMEs to benefit from shared tools they can adapt to their content policy. However, not all companies are equally affected by the problem. For example, a small company headquartered within the EU[36] emphasised during the public consultation that it had tried to set up a content moderation system with an investment as high as half the staff, but, with no incidence of illegal content, it had to repurpose scarce resources.

At the same time, there is a recurrent criticism of the existing systems implemented by the hosting services providers regarding the lack of sufficient safeguards and the limitation to users' rights through erroneous removal of legal content or suspension of accounts. Both the Communication and the Recommendation raise these issues and call on companies to set up reliable safeguards for over-removal of lawful content. Calls have been made not only for the establishment of complaint procedures (counter-notices) and/or increased clarity around these, but also for future reports to quantify the removals and the outcomes of complaints.[37]

Academics[38] submitting replies to the open public consultation have pointed to the lack of real incentives (apart from sporadic media attention) companies might have to deal with counter-notices, whereas non-treatment of notices can more easily lead to legal and financial consequences. They also

34 The most recent report involved the misidentification of an article about the US Declaration of Independence as hate speech, https://www.telegraph.co.uk/news/2018/07/05/facebook-censors-americas-declaration-independence-hate-speech/

35 Encryption on the server, different from end-to-end encryption for transmission of the data through the network. For encryption on the server, the hosting service does not have itself the encryption keys and this is generally handled by the customer only who can share the content and relevant encryption keys with third parties.

36 Offering data storage and Platform-as-a-Service cloud services

37 *VOX-Pol Blog*, 4 April; The Santa Clara Principles on Transparency and Accountability in Content Moderation, 7 May, 2018.

38 E.g. contributions from Tilburg University, or feedback on the IIA from Stanford University



www.parlament.gv.at

underlined that existing counter-notice procedures are by and large underused, with the few companies who do report on counter-notices listing on a yearly basis only one-to-two digits numbers.39

In addition, a rich literature is emerging on the need for specific safeguards for algorithmic decision-making, where biases and inherent errors and discrimination can lead to erroneous decisions. This was particularly flagged by academics in the feedback on the Inception Impact Assessment, pointing to the plausible impacts on vulnerable groups.40

**Stakeholders' views**

Regarding notice and action procedures, the 2018 Eurobarometer on illegal content reported that :

- 33% of the individual respondents have seen allegedly illegal content and have reported it to the hosting service;
- over 83% of them found the procedure easy to follow;
- 30% of the respondents whose content was in their view wrongly removed41 had issued a counter-notice;
- 64% of the respondents whose content was removed found both the content removal process, and the process to dispute removal not to be transparent;
- 8% of the respondents said their content had been wrongly removed (self-reported) by a hosting service, including on false grounds of terrorist content or child sexual abuse, but mostly for claims of IPR infringements;
- 27% claim to have contacted the hosting service and contested the decision.

### *2.4.4. Hosting services providers' policies to detect, assess and remove content are not transparent for users and public authorities to monitor companies' action against terrorist content.*

The Communication on illegal content identified a general lack of transparency on online platforms' content and removal policies, as well as a lack of detailed data on their removal decisions. The Commission's Recommendation called for further measures to inform both users as well as public authorities. Transparency is needed to be able to assess the full breadth of the problem and the impact of efforts, to provide the necessary public assurance that sufficient mitigating measures are being taken to protect citizens against illegal online activity, as well as to capture the necessary evidence for investigative and prosecutorial purposes.

The voluntary dialogues for the different types of illegal content have significantly improved the reporting on the advances made by hosting services providers and notice providers, not least though the alignment of reporting indicators and some comparable frequency of measurements42. However, this is necessarily limited to the service providers joining the dialogues.

Furthermore within those dialogues, reporting has not always been followed-up with consistently. For instance on terrorist content online, the EU Internet Forum developed a set of indicators in order to improve transparency in this area and better track progress. Whilst first rounds of reporting ensured greater transparency in relation to how those who responded are addressing this problem, only approximately 14 out of the 33 companies that were invited to provide data, responded. This figure accounts for just a fraction of the overall number of platforms which are reportedly being exploited for terrorist purposes.

39 ICF study (forthcoming). Comparative analysis of transparency reports of several companies points to negligible numbers of counter-notices per year.

40 E.g. https://www.theguardian.com/technology/2017/jan/18/facebook-moderation-racial-bias-black-lives-matter In the feedback received, special attention is given to posts in Arabic or legitimate speech on Islam and it is flagged that special care is needed not to build catch-all moderation systems overly-preventive for specific communities.

41 N=1636 respondents who claim their content was wrongly removed

42 See, for example **Error! Reference source not found.**, *supra*, p.12



www.parlament.gv.at

Beyond the voluntary dialogues, only a relatively limited number of intermediaries publish transparency reports43. While they offer some level of understanding on the company's actions, they are rarely granular enough to inform policy-makers or law enforcement on the evolution of illegal content online and they are not comparable. The reports generally present limited data, sometimes in absolute values, on the notices received, content taken down and, in even fewer instances, the counter-notices and shares of content reinstated after takedown. Importantly, they rarely distinguish with precision the types of illegal content beyond copyright infringements and content signaled through 'government notices'. Recent developments include YouTube's report[44] on the enforcement of its community guidelines, presenting also data on proactive measures to take down terrorism content or child abuse; Telegram publishes an (API accessible) daily report on the number of ISIS channels and bots taken down. In the open public consultation, only one third45 of the users who notified content received information about the course of action taken by the hosting service. For organisations flagging content, the solution adopted is generally a monitoring system including regular checks of the URL until the content is taken down. However, while they provide an external check in the process, such systems are not resource-efficient neither for the flaggers (cost of setting up the system), nor for the hosting service (generating unnecessary traffic and network congestion), and run the risk of blocking for suspicious network activity.

**Stakeholders' views**

According to the open public consultation, nearly half of the individuals who had notified content did not receive any information from the service regarding the notice, and one third reported to have been informed about the follow-up given to the notice. For one fifth, the content was reported to be taken down within hours.
One fifth46 of the respondents who had their content removed from hosting services reported not to have been informed about the grounds for removal.

In terms of removals, out of those who claimed in the open public consultation that they reported illegal content, 7% say the content was kept online, while 22% say it was taken down. Out of those who responded in the Eurobarometer data collection, 45% says the reported data was removed, while 20% says it was kept online. Further 7% says that the content was kept online but with more restricted access, while 8% said that it was kept online but was slightly modified.

## 2.5. What are the consequences of the problem?

Availability of terrorist content online can accelerate the radicalisation process, recruit terrorist supporters, and galvanise, facilitate and instruct terrorist activity. Organisations such as Daesh, Al Qaida and others have used the internet to promote their ideology, groom and recruit, and more recently, to incite, train and provide instructions for carrying out terrorist attacks through the use of detailed online magazines and manuals. According to research conducted by VOX-Pol on a set of UK-based convicted terrorists, "a third (32%) prepared for their attacks by using online resources". "More than half (54%) of all actors used the Internet to learn about some aspect of their intended activity", a figure which has increased over time up to 76%, which could be an indication of increased use of the internet by would-be terrorists or of increased availability of terrorist material online. In the aftermath of terrorist attacks, terrorists use the internet to glorify in their atrocities and urge others to follow suit.47

43 Google started publishing a transparency report in 2010, and the practice was followed by a small number of companies, mostly reflecting DMCA-related takedowns. The Google Transparency Report publishes a list of services that usually issue transparency reports: https://transparencyreport.google.com/?hl=en.
44 https://transparencyreport.google.com/youtube-policy/overview?hl=en
45 990 individuals
46 450 out of nearly 2000
47 For a detailed summary of terrorist content online, see Annex 9.

Some anecdotal cases also point to examples where it appears that perpetrators of terrorist attacks have been radicalised solely through the internet. For instance, in Denmark in 2017, a teenage girl was found guilty of attempted terrorism for having tried to make bombs to be used in terrorist attacks against her own former local school and against a Jewish school in Copenhagen. The girl became radicalised via the internet and chat contacts within just a few months[48].

The nature of content might be different but terrorist content poses a serious harm to victims and the society more generally. Images of murder and torture of terrorists' victims, such as the immolation of the encaged Jordanian pilot in 2015 by Daesh, are For the general public who happen to fall upon this material, and for the victims and their relatives, this material can be extremely distressing. However, not all terrorist content is necessarily violent. Often, particularly in the early grooming stages, terrorists' will use a softer approach. Since early 2017, Daesh has even resorted to using cartoons to glorify and promote their ideology to young children with the intention of indoctrination. For the curious user, such material has the potential to groom and recruit. And for those who have the desire to inflict harm and commit terrorist acts, terrorist material can be used to galvanise them into action (as was the case with the attack on the Thalys train in August 201549), and equip them with the capability and know-how to convert that intent into devastating action.

With regards to consequences of response measures, flaws in content removal procedures can lead to unintended removal of legal content, also to minimise exposure to legal or financial consequences, as such, any regulatory incentives need to be appropriately balanced with safeguards to ensure freedom of speech is protected.

Another consequence of the problems is the inability of public authority to monitor the evolution of the problem, as insufficient data prevents public authorities to assess the effectiveness of current procedures to detect and remove illegal content, as well as their impact on public and private interests.

Finally, the overall consequence of the problems collectively is a lack of trust in the online environment, which limits the growth and innovation capacity of hosting services providers in the Digital Single Market.

## 2.6. How will the problem evolve?

Without action, the problem of terrorist content online would persist to different degrees, depending on the effectiveness of the different measures already in place to curb its dissemination.

While terrorist content originating from organisations such as Daesh might be forced increasingly to smaller platforms as a result of reinforced content moderation policies, it is likely that terrorist organisations will continue to seek innovative way to exploit the reach of large platforms, in parallel with disseminating content on smaller ones.

Therefore, hosting services would continue to be abused for the dissemination of illegal content, in particular those who do not participate in the voluntary dialogues, or those who do not comply with the Recommendation on illegal content. Although the voluntary process would expand, it is unrealistic to expect that all platforms which host illegal content would join the current voluntary process, or indeed take heed of the Recommendation. The spreading and reappearance of content

48 Europol TE-SAT report 2018

49 According to the Paris prosecutor, the internet history on Ayoub el-Khazzani's phone shows that after he boarded the train, Khazzani listened to a “YouTube audio file in which the individual exhorted his followers to raise arms and fight in the name of the prophet.”



www.parlament.gv.at

across platforms would continue. The uneven application of procedures to detect and remove illegal content would likely continue, given the non-binding nature of the Recommendation. The ability of authorities and policy-makers to monitor the evolution of the problem, and for users to understand content moderation principles would remain patchy – with those platforms participating in the voluntary dialogues providing more information than those who do not.

At the same time, a series of recent and forthcoming legal instruments are expected to bring further clarity and give legal incentives to some types of services providers to act against terrorist content they host. In particular, the revised Audio-Visual Media Services Directive would require video-sharing platforms whose principal purpose or essential functionality is the provision of audiovisual content to take a series of measures to protect the general public from terrorist content, as well as from illegal hate speech, and CSAM, and to protect minors from harmful content. Measures expected to be put in place by services include prohibiting such content through their Terms of Service, flagging mechanisms available to users and feedback to users on the follow-up of the notices, as well as complaint and redress mechanisms for users in case of disputes over the application of the envisaged measures (i.e. counter-notices). Even though not directly imposing obligations on hosting service providers, the measures implemented by Member States under Article 21 of the Terrorism Directive will ensure that material that amounts to public provocation to commit a terrorist offence will be removed (e.g. in the context of a criminal investigation). However, action by Member States alone to refer or block material, will always fall short considering it is the companies who are best placed to know which technology can be applied and how in order to ensure a safe online environment for their users. Nor would this approach achieve an effective EU-wide approach with regards to securing the removal of terrorist material for preventative efforts.

## 3. WHY SHOULD THE EU ACT?

### 3.1. Legal basis

As far as EU action may take the form of a legislative proposal in the area of terrorist content, the legal basis depends on the primary objective and scope of the proposal. Given the problems that this Impact assessment is addressing and the solutions proposed, Article 114 TFEU is the most appropriate legal basis for an EU intervention. In general, in the field of terrorist content online, the legal basis could be found mainly either in Article 114 TFEU (approximation of laws for the improvement of the internal market) or in Article 83 TFEU (judicial cooperation in criminal matters for the definition of criminal offences).

According to Article 114 TFEU, the European Parliament and the Council shall adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.

Following well-established case-law of the CJEU50, Article 114 is the appropriate legal basis to address differences between Member State provisions which are such as to obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market, and a possible legal basis for measures to prevent the emergence of future obstacles to trade resulting from differences in the way national laws have developed. As the Court has said, the EU 'legislature cannot be

50 See, C-380/03 Germany v European Parliament and Council, judgment of 12 December 2006.



www.parlament.gv.at

prevented from relying on that legal basis on the ground that the protection of other policy objectives is a decisive factor in the choices to be made.'51

Recourse to Article 114 TFEU as a legal basis does not presuppose the existence of an actual link with free movement between the Member States in every situation covered by the measure founded on that basis. To justify recourse to Article 114 TFEU as legal basis what matters is that the measure adopted on that basis must actually be intended to improve the conditions for the establishment and functioning of the internal market52.

Article 114 TFEU can also be used to impose obligations on **services providers established outside the territory of the EU** where their service provision affects the internal market, when this is necessary for the desired internal market goal pursued. For instance, the Regulation on Geoblocking53 or the Proposal for a Regulation on promoting fairness and transparency for business users of online intermediation services54 consider that the ultimate effect of the instrument would be undermined if the geographic scope was limited to services providers established in the EU.

Finally, Article 114 TFEU can also serve as a legal basis to impose an obligation to third country companies to **appoint a representative** within the territory of the Union, insofar as this is merely incidental with regard to the main purpose or component of the act. This is the case, for instance, for the NIS Directive55, exclusively based on Article 114 TFEU.

According to Article 83(1) TFEU the European Parliament and the Council may establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension such as terrorism. Article 83(2) TFEU provides that if the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures, directives may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned.

In view of the problems to be addressed, Article 83 seems to be a less appropriate legal basis for an EU intervention, as the analysis does not conclude on the need for 'establish[ing] minimum rules concerning the definition of criminal offences and sanctions', but rather for harmonization of conditions for hosting service providers to provide services cross-border in the Digital Single

51 See C-380/03 Germany v European Parliament and Council, judgment of 12 December 2006, where the policy objective at hand was public health protection.

52 Ssee, to this effect, Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-4989, paragraphs 41 and 42, and Case C-101/01 Lindqvist [2003] ECR I-12971, paragraphs 40 and 41.

53 Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC: " The effects for customers and on the internal market of discriminatory treatment in connection to transactions relating to the sales of goods or the provision of services within the Union are the same, regardless of whether a trader is established in a Member State or in a third country. Therefore, and with a view to ensuring that competing traders are subject to the same requirements in this regard, this Regulation should apply equally to all traders, including online marketplaces, operating within the Union"

54 https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services: Since online intermediation services and online search engines typically have a global dimension, this Regulation should apply to providers of those services regardless of whether they are established in a Member State or outside the Union, provided that (…) business users or corporate website users are established in the Union (and) business users or corporate website users offer their goods or services to consumers located in the Union.

55 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union " Where a digital service provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such a digital service provider is offering services within the Union, it should be ascertained whether it is apparent that the digital service provider is planning to offer services to persons in one or more Member States."

Market. The intervention would not seek to harmonise criminal content, as the Terrorism Directive, nor obligations under criminal proceedings.

### 3.2. Subsidiarity: necessity of EU action

According to the principle of subsidiarity laid down in Article 5(3) of the Treaty, action at EU level should be taken only when the aims envisaged cannot be achieved sufficiently by Member States alone and can therefore, by reason of the scale or effects of the proposed action, be better achieved by the EU.

Several Member States have legislated56 in the field of removal of illegal content online in relation to aspects such as notice and action or transparency. However, the internet is by its nature cross-border, and content hosted in one Member State can normally be acceded from any other Member State. The need to ensure public security at national level has to be balanced with the fundamental freedom of provision of services and freedom of establishment in the Internal Market, which justifies the existence of derogations to that freedom for reasons of public security. Public security has a particular importance in the area of terrorism, given the gravity of the risks involved. In principle, the place of establishment should not be a barrier to provide services across the EU (subject to derogations, as long as justified, proportionate and necessary).

As a result of this, a patchy framework of national rules is appearing and risks to increase, which would jeopardise an effective exercise of the freedom of establishment and the freedom to provider services in the EU (see 2.4.1). Intervention at national level cannot solve this problem. This justifies the need for EU action, as echoed by the Council Conclusions of June 2018 inviting the Commission to present a legislative proposal in this area.

### 3.3. Subsidiarity: added value of EU action

The different and diverging legal regimes applicable to online intermediaries increase compliance costs while also being the source of legal uncertainty on the qualification of the content as illegal content and on the scope of responsibilities and obligations for service providers, raising a serious concern among operators. As representatives of the industry have stated during consultations, diverging requirements in different Member States impose compliance with diverging regulations, or there is a risk that new regulations would do so. In addition, the effects of any action taken under national law would be limited to a single Member State.

EU action reducing compliance costs, allowing their predictability and enhancing legal certainty would ensure that hosting service providers' actions against terrorist content online can be streamlined and scaled up increasing its effectiveness. This would allow more companies to take action strengthening the integrity of the digital single market. EU action in this area would ensure a coherent approach applicable to online platforms operating in all Member States.

Action at EU level would be only partially effective if it was limited to hosting services providers established in the EU. This would create a competitive disadvantage vis-à-vis companies established in third countries, which would not be subject to any compliance costs in this regard. Furthermore, the effect in the availability of terrorist content online would be only limitedly achieved.

56 Finland, France, Greece, Hungary, Italy, Lithuania, the United Kingdom, Spain, Sweden, and most recently in Germany, see Annex 8.



www.parlament.gv.at

Due to the interest of companies outside the EU to continue providing its services within the Digital Single Market, the EU can act as a standard-setter for measures to combat terrorist content online globally.

## 4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

### 4.1. General objective

The general objective is to establish uniform rules to prevent the misuse of hosting services for the dissemination of terrorist content online in order to guarantee the smooth functioning of the Digital Single market, with high levels of trust and security.

### 4.2. Specific objectives

*4.2.1. Facilitate the provision of online services across the DSM by limiting further legal fragmentation*

The first specific objective is to ensure a predictable, harmonised legal framework on the obligations related to handling terrorist content required from hosting service providers when providing their services cross-border. This would bring legal certainty and allow companies to streamline processes, limiting compliance costs with fragmented rules.

*4.2.2. Increase the effectiveness of measures to detect, identify and remove terrorist content*

The second specific objective is to ensure greater effectiveness of the mechanisms to reduce availability of terrorist content in the EU, in particular by ensuring that hosting service providers and national authorities take appropriate, effective and proportionate actions against the spread of terrorist content.

*4.2.3. Increase transparency and accountability of hosting services for measures taken to detect, identify and remove terrorist content*

The third specific objective is to ensure that both citizens, and in particular Internet users, and public authorities have sufficient information to appraise the actions taken by hosting service providers to detect, identify and remove illegal content.

*4.2.4. Improve the ability of relevant authorities to intervene against terrorist content online and to combat crime*

A fourth specific objective relates to enabling public authorities to exercise effective action against the dissemination of illegal content online and take appropriate action including investigations into the underlying criminal offences.

*4.2.5. Safeguard against the risk of erroneous removal of legal content and ensure protection of fundamental rights*

A fifth specific objective is to provide for appropriate measures to safeguard against erroneous removal of legal content and ensure the effective exercise of fundamental rights online.



www.parlament.gv.at

## 5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

### 5.1. What is the baseline from which options are assessed?

In the baseline scenario, reactive measures will continue to be carried out in the framework set out by the E-commerce Directive and the liability regime set out therein, under which hosting service providers are under certain conditions exempted from liability for the illegal content they store.

The Directive on Combating Terrorism should be transposed into national laws by September 2018, and obliges Member States to "*take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence*". As clarified in recital 21, the Directive leaves Member States a wide margin of discretion as to the form of removal measures, stipulating that these may take the form of legislative, non-legislative or judicial action and that it is without prejudice to voluntary action taken by the internet industry. Information transmitted to the Commission so far indicates divergence between the transposition of the measures between Member States. The transposition is a mix of notice and takedown actions under the general framework of Directive 2000/31/EC and measures based on criminal law, often constituting general competence of seizure of illegal content. Although such measures seem to meet the requirements of the Directive, they are unlikely to result in a significant reduction of the volume of terrorist content online.

Furthermore, the Audio-visual Media Directive's transposition into national law would similarly be completed by end 2020, obliging Member States "*to ensure that video-sharing platform providers under their jurisdiction take appropriate measures to protect […] the general public from programmes, user-generated videos, and audiovisual commercial communication [containing] a public provocation to commit a terrorist offence, [as well as] child pornography, […] racism and xenophobia."*

The Recommendation on measures to effectively tackle illegal content online can also be expected to bring further results, not least in what concerns detecting, notifying, and removing illegal content online, as well as detailed transparency reporting requirements. However, given the non-binding nature of the Recommendation, the adoption of the measures relies on the voluntary action of a limited number of companies and is unlikely to effectively tackle and keep up with the changing online operations from terrorist organisations.

Under the baseline, the implementation of current non-regulatory measures would continue and evolve. The cooperation between industry, Member States, Europol and the Commission under the EU Internet Forum would be pursued and would be reinforced. Efforts would focus both on expanding the number of companies participating, and on following up and supporting further commitments from companies and sharing of tools and best practices. In particular, some companies, mainly major ones, would continue to develop and use proactive measures, such as human review combined with automated detection tools. Gradual expansion of the use of the filtering database developed by industry currently used by 13 companies up from 4 last year can also be expected; and company initiatives such as the Global Internet Forum to Counter Terrorism would also continue to reach out to new companies.

Further R&D&I support would reinforce the financing of research projects and networks such as VoxPol, which help better understand the evolving threat of terrorist content online. Such research has been very valuable in the past in designing targeted regulatory and non-regulatory responses and has helped hosting service providers and public authorities to keep track of the nature of the problem.



www.parlament.gv.at

National laws in the area of illegal content can be expected to continue to evolve. The German NetzDG, which covers hate speech and some elements related to terrorist content, has entered into force on 1 January 2018, and first transparency reports are expected by July 2018. The French government has similarly been reported to consider a dedicated law on hate speech.

**Stakeholders' views**

Member States representatives in the E-Commerce Expert Group supported the ongoing collaboration under European and national-level cooperation with hosting service providers and considered that the measures to implement the Recommendation are ongoing. Horizontal instruments at EU level would hence not be needed yet. Furthermore whether under the Open Public Consultation, or the high-level meeting with a wide range of companies in January 2018, stakeholders raised the preference for targeted intervention on specific issues of particular public value.

On terrorist content, Member States representatives noted that the EU Internet Forum has generated important progress and good results within a short period of time. However, they also highlighted shortcomings and that results (in terms of effective and swift removal and proactive measures by companies) did not match the challenge at hand. A number of Member States called for legally binding obligations to speed up progress, ensure sustainable results and compliance by a larger number of companies. Other Member States highlighted that more time was required to fully assess progress before deciding on legislation.

Hosting services, as reported in the public consultation and targeted consultations, do not consider that additional regulatory intervention would be conducive to better tackling illegal content online, highlighting the general cooperation and good results in the actions taken through the sector specific voluntary dialogues. Civil society organisation advocating digital rights are also in favour of maintaining the baseline option. Associations representing large numbers of hosting service providers stated that, if legal instruments are envisaged at EU level, they should in any case be problem-specific and targeted whilst broadly supporting further harmonisation of notification information. Different companies highlight the different available capabilities across businesses, as well as the different incentives and technical possibilities depending on their value propositions. Caution was expressed as to proactive measures and the feasibility of establishing strict time limits on takedown of content from upload, pointing to burdens for SMEs, and to incentives for over-removal. Companies were also generally open to cooperation especially with government agencies or law enforcement flagging illegal content.

In the Eurobarometer, the overwhelming majority of respondents agreed that arrangements need to be put in place to limit the spread of illegal content online, and that, at the same time, freedom of expression needs to be protected. In the open public consultation, respondents were asked to scale the importance of having such measures in place, and to protect freedom of expression online, respectively; they considered overall that the protection of freedom of expression as a more important measure.

In the Open Public Consultation, 30% of respondents considered that the current legal framework for tackling each of the different types of illegal content was effective and nearly 40% found that actions currently taken by hosting service providers are effective. At the same time, 60% expressed that different types of illegal content should be dealt with in different legal frameworks, to take into account specificities, while 12% disagreed with this.

## 5.2. Options discarded at an early stage

A number of options were considered early in the analysis process and discarded against effectiveness, coherence and proportionality criteria:

1. **Transformation of the Recommendation on measures to effectively tackle illegal content online into binding rules across all types of illegal content**

   In this option, the provisions of the Recommendation would be made legally binding. However, preliminary assessment against the set objectives points to an unnecessary and disproportionate intervention, and raises concerns in particular as regards the necessity to establish generalised requirements for proactive measures to detect and remove all types of allegedly illegal content, amounting to a general monitoring of the content uploaded by users of hosting services.

   Moreover, the specificities of the different types of content need to be acknowledged and treated accordingly, including regarding the effectiveness and evolution of the current voluntary measures.



www.parlament.gv.at

Hence, to date, such policy option is not suited for a 'one size fits all intervention' and does not appear necessary and proportionate and would not justify a potential interference with fundamental rights, in particular, with freedom of expression and information, data protection and freedom to conduct a business and compliance with the existing legal framework, in particular the E-Commerce Directive.

**2. Harmonised rules across all types of illegal content clarifying notice-and-action procedures**

A harmonised legal approach to all categories of illegal content, including terrorist content, CSAM, illegal hate speech, content infringing intellectual property rights, but also content rendered illegal in national law, could cover notice-and-action procedures, as clarified in the Recommendation. This could include an obligation for hosting service providers to put in place an easy to access mechanisms for submissions of notices by electronic means, as well as easy to access complaint mechanisms for content providers supported by the obligation to inform content providers when their content is taken down. The option would also include minimum quality requirements for submitted notices, and transparency obligations through annual reports, as well as sanctions for systematic non-compliance with the obligations. This instrument would be applicable to hosting service providers who offer/direct their services to users residing in the Union, irrespective of their place of establishment.

While the option would be proportionate and would have limited interference with fundamental rights, it would have only a limited impact in addressing the objective to increase the effectiveness of measures to detect, identify and remove terrorist content and to improve the ability of the authorities to intervene against terrorist content, compared to the evolving baseline. The limited effect is specific to terrorist content, not least due to the specific behavioural patterns in the dissemination of the content, as well as the expected transposition and enforcement of the revised AVMS Directive, already establishing grounds for such measures in the case of video-sharing platforms. In addition, the Recommendation gives guidance on such horizontal measures, and should bring further certainty and relief to hosting service providers. The option is therefore discarded at the current stage, as it does not sufficiently address the policy objectives, without precluding potential benefits such a measure could bring in the future, depending on the evolution of the baseline for all types of illegal content.

**3. Enhanced voluntary approaches**

There have been several Member States and stakeholders advocating continued or enhanced efforts under the voluntary arrangements within the EUIF. The current voluntary arrangements within the EU Internet Forum could be further strengthened by developing a Memorandum of Understanding or a code of conduct together with companies and Member States setting out more specific commitments from companies in terms of e.g. specific timeframes for removal of content as well as proactive measures to avoid the dissemination of terrorist content in particular across different platforms. However, the reliance on commitments from companies, the limited outreach (only a small fraction of affected service providers have engaged in the EUIF), the limited level of progress when compared to the scale of the problem, developments and the need to significantly reduce accessibility to terrorist content as a matter of urgency reveal the limits of the voluntary approach. A further continuation or strengthening of the voluntary approach was therefore discarded as not being sufficient for tackling terrorist content.



www.parlament.gv.at

4. **Revising the E-Commerce Directive:** the revision of the framework conditions set in the E-Commerce Directive for the obligations on information society services in the removal of illegal content could create further legal incentives for hosting service providers to remove terrorist content, but would not address the objectives of the intervention, nor would this address convincingly and proportionately the drivers of the problem. The balance achieved by the current provisions in protecting fundamental rights, in particular the freedom to conduct a business and freedom of expression, would also be jeopardised. In addition, the measure would not be aligned with the Digital Single Market's Strategy concerning online platforms, as presented in the Communication on online platforms57, and would be disproportionate as to the small share of hosting services abused by terrorist content.

5. **Amending the Terrorism Directive:** a targeted amendment of Article 21 to further specify obligations on Member States in relation to the removal of terrorist content online could lay down more specific rules on procedures to request removal of terrorist content including possibly an extension of the type of activities/material that should be covered by such obligations (i.e. extension from currently only incitement to terrorism to other offences). However, the focus on criminalisation of terrorist offences as opposed to purely preventative measures, the geographical limitations and limitations in terms of safeguards and other flanking measures (which would not have been possible under this legal basis) would have meant that the initiative would have had limited impact on the objectives of preventing the dissemination of terrorist content under harmonised rules for the cross-border provision of services in the Internal Market and thereby increasing trust in the Digital Single Market. An amendment of the Terrorism Directive was therefore discarded given the limited impact on the overall objective.

## 5.3. Intervention logic and options retained

The abuse of hosting service providers for spreading terrorist content online follows a specific pattern, outlined in Section 2.3, involving a range of hosting service providers of different size, audience and reach. Although voluntary processes under the EU Internet Forum have led to demonstrable progress amongst those companies who participate, it continues to be easy for terrorists to spread content online. Only 14 companies out of 33 contacted in the context of the EU Internet Forum cooperated with the reporting following the Recommendation, while Europol has identified more than 150 hosting service providers as being particularly exposed to terrorist content. The scale and pace of progress among hosting service providers as a whole is not sufficient to adequately address the rapidly evolving problem.

At the same time, the likelihood of new attacks in the EU by jihadist terrorists remains high58, and online propaganda and networking via social media continue to be essential means by which to recruit and radicalise terrorists. In almost every attack that has occurred, the perpetrators have either used the internet by way of preparation or even in the delivery of the attack, and supporters have glorified the acts in the aftermath and urged others to follow suit.

In light of the urgency to act against the spread of terrorist content online59, as well as the limits of the voluntary processes, the retained options are all of a legally binding nature. They build on the

57 COM(2016) 288.
58 Europol EU Terrorism Situation and Trend Report TE-SAT 2018, version of 20 June 2018, https://www.europol.europa.eu/sites/default/files/documents/tesat_2018_0.pdf
59 Detailed *supra*, section 2.1 Scope and further context, p. 7



www.parlament.gv.at

evolving baseline and additional supporting measures, and include a series of building blocks – with different intensities of intervention – to tackle the problem drivers and pursue the specific objectives.

The intervention logic presents how the building blocks included in the options address the specific objectives and the problem drivers is based on: Provisions to **harmonise the procedures for removal or disabling access to terrorist content** following a removal order from a national authority (giving effect to Article 14 (3) of the E-Commerce Directive). To enable the procedures, harmonisation further includes a **common definition of terrorist content online**, as well as clarity concerning **judicial redress** available to hosting service providers and content providers against removal orders. These provisions would limit further legal fragmentation and reduce costs of operations for hosting service providers, not only in line of a standardised process they are exposed to when receiving removal orders, but also in relying on accurate and clear orders, allowing for swift removal. The quality of removal orders and the smooth process would also increase the overall effectiveness in the removal of terrorist content.

Provisions to ensure **transparent processes and reporting** to authorities and the Commission, would increase the accountability and trust in the content moderation process, and would support policy-makers and national authorities in combatting terrorist content and would allow users to better understand how hosting service providers apply their content management policies.

**Cooperation across national authorities and Europol** would improve their ability to act collectively against terrorist content, avoiding duplication, and would reduce complexity and costs on hosting service providers in interacting with national authorities when offering their services cross-border.

In addition, provisions to ensure that, in those cases where companies are exposed to terrorist content, the hosting service providers put in place **appropriate and proportionate measures to proactively detect terrorist content**.

**Safeguards** and provisions to ensure that measures taken to detect and remove terrorist content do not lead to erroneous over-removal of legal content and comply with fundamental rights.

Provisions **to ensure that measures are enforceable**, including the establishment of legal representatives for non-EU companies, establishing points of contact and ensuring Member States have a coherent set of sanctions in place.

The figure below summarises the intervention logic.



www.parlament.gv.at

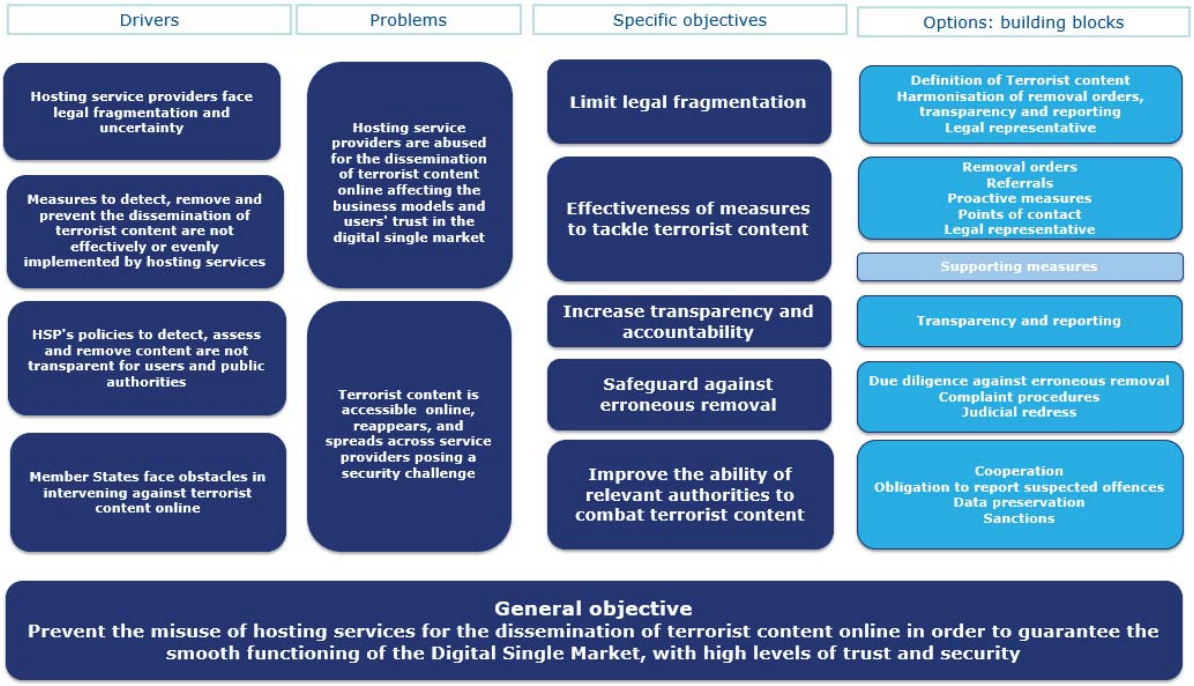



***Figure 3*** *Intervention logic. Building blocks summarise the types of actions, but the three options and related options include variations in the design and scope of the actions.*

## 5.4. Description of the policy options

The report presents and assesses three policy options. The common elements, as well as the main differences are presented below. Table 2 presents in a comparative format the respective measures under each option

***Main measures under all options***

All options have in common the creation of a new, harmonised system of removal orders for terrorist content online from national authorities, upon which hosting services must act within one hour. This system is based on a clear legal definition or what constitutes terrorist content. Such a definition would be aligned as closely as possible to the relevant provisions of the Directive on Combatting Terrorism.60 The assessment of the content would need to account for factors such as the nature and wording of the statements, the context in which the statements were made including whether it is disseminated for educational, journalistic or research purposes and the potential to lead to harmful consequences. These orders should not require any assessment on the part of the hosting service providers, but would be subject to judicial redress. Safeguards, notably information to content providers, complaint procedures and judicial redress as well as other provisions to ensure that measures taken to detect and remove terrorist content do not lead to erroneous over-removal of legal content to ensure compliance with fundamental rights are also common to all options, including a general due diligence requirement to avoid erroneous removal of legal material.

Further, all options have in common a number of reporting obligations in the form of publishing transparency reports, reporting on the measures taken to Member States and the Commission, as well

60 As to the material scope, the dissemination of terrorist propaganda as such is not explicitly mentioned as a criminal offence under the Directive on Combatting Terrorism, not is terrorist propaganda defined as such. However, the Terrorism Directive contains offences that can be committed both offline and online. Therefore, the dissemination of material over the Internet that amounts to public provocation to commit a terrorist offence, recruitment and training for terrorism would constitute a criminal offence when committed intentionally



www.parlament.gv.at

as notifying authorities of suspected criminal offences. In addition, cooperation obligations between national authorities, hosting service providers, and where relevant Europol are also foreseen.

The scope of these obligations in all three options would focus on all hosting service providers (personal scope) established in the EU and in third countries - insofar as they offer their services in the Union (geographic scope) - based on the above-mentioned definition of what constitutes terrorist content (material scope). Given the nature of the problem and the need to avoid the abuse of smaller platforms, no exemptions are foreseen for SMEs under any of the options.

All options would foresee sanctions as well as requirements to establish a legal representative in the EU for companies established outside the EU. Such a legal representative would ensure enforceability of EU rules for hosting services established outside the EU.

***Main differences***

The main differences between the three options are as follows:

*Material scope*

- Option 1 would limit the material scope to content disseminated to directly incite to commit a terrorist act, following a **narrow definition.**
- Options 2 and 3 would cover material disseminated to incite, recruit and train for terrorism closely linked to the terrorist offences as stipulated in the Terrorism Directive.

*Harmonisation of procedures governing referrals*

Option 1 would not regulate Referrals in a legal text, while in options 2 would introduce obligations for hosting service providers to have procedures in place for treating referrals received from Europol and option 3 would additionally include those of Member States. Furthermore feedback on action following referrals would need to be provided to Europol (option 2 and 3) and MS (option 3). This would not entail a requirement for take down.

*Requirements to Member States:*

- Options 1 and 2 require Member States to designate competent authorities
- Option 3 requires Member States to establish competent authorities with capacity to detect and notify terrorist content
- To ensure coordination and avoid duplication of removal orders, in options 2 and 3 Member States would be obliged to inform, coordinate and cooperate with each other with regards to removal orders (option 2 and 3), but also referrals (option 3), and would have the possibility to channel removal orders and referrals via Europol.

*Proactive measures*

Under all three options, provisions related to proactive measures would only apply to a subset of hosting service providers, i.e. those exposed to terrorist content, based on objective criteria. Estimates situate the number of hosting services concerned in between 150 and 40061.

The scope of specific proactive measures ranges across the three options, as follows:

- Option 1, where a risk assessment is required, as a basis for potential voluntary measures;
- Option 2, where hosting service providers are required to draw up an action plan to tackle terrorist content, proportionate to the level of risk, which may include the deployment of automated tools for the prevention of re-upload of already removed and identified material;

61 *Supra*, p. 7



www.parlament.gv.at

- Option 3 includes more comprehensive proactive measures requiring service providers to detect also new material, in all instances the scope being proportionate to the level of exposure to terrorist material as well as the economic capacities of the service provider, where appropriate.

*Data preservation requirements*

In addition to the reporting obligations for suspected criminal offences, included in all options, option 3 would require service providers to ensure data preservation as a safeguard in cases of erroneous removal as well as to ensure the existence of evidence for any potential criminal investigations, with the appropriate safeguards to comply with the obligations under the General Data Protection Regulation

***Supporting measures***

In addition to the legal provisions, either one of the three legislative options would be accompanied by **a series of supporting measures**, in particular to facilitate cooperation across national authorities and Europol, as well as the collaboration with hosting service providers, and R&D&I support for development and take-up of technological solutions. In particular, near-real-time information transmission across authorities on removal orders and referrals would bring further efficiency for the authorities and limit burden on HSPs in dealing with such notices. A cooperation platform could be further developed and managed by Europol, in line with its mandate. Further functionalities could lead to the creation of a publicly run, high-accountability automatic system to further enhance the expeditious takedown of terrorist content and curb its dissemination across platforms. This electronic infrastructure would be accessible to companies on a voluntary basis.

Additional awareness-raising instruments for SMEs could be deployed following the adoption of the legal instrument, as well as specific training and information from Europol, in collaboration with the national authorities.

**Stakeholder views:**

In a targeted questionnaire addressed to the Member States, to which the Commission received 19 responses, the Member States considered the following measures as necessary or very necessary: access to content removed by companies for law enforcement purposes, reporting by companies, a common definition of terrorist content, a sanction mechanism, points of contact established by companies, tools for companies to detect content already identified as terrorist material, requirements for action upon referral and for proactive measures by companies, safeguards, transparency reports, requirement for Member States to establish referral capabilities.

At the same time, they highlighted risks that need to be taken into account: burden of creating oversight and dispute resolution mechanisms, the need to adapt measures to changing modus operandi of terrorists and evolution of technology, the need to address companies on a global level, need to balance fundamental rights concerns.

Timeframes for removal were seen as important during the targeted consultations with Member States, in which some noted that a one hour removal time was seen essential, especially on content which is referred by a competent authority. Additionally, in replies to the open public consultation non-for-profit organisations identifying and reporting allegedly illegal content online noted that the setting of time limits to processing referrals and notifications from trusted flaggers would be useful to support cooperation between hosting services providers and trusted flaggers.

While many stakeholders in the OPC favoured the continuation of the baseline, they pointed the need of ensuring any intervention of a legislative nature should take into account the specificities of different types of content. Some of the consulted companies highlighted that they see value in an unambiguous definition of



www.parlament.gv.at

terrorist content across the EU. In line with answers to the OPC, many companies were not in favour of further obligations, however one noted that it would be positive, as long as it is proportionate to the size of the platform. Concerns were voiced over strict timelines should the content be assessed and reviewed prior to removal. On proactive measures a number of concerns were expressed as to the feasibility of these measures for smaller companies and noted the additional burden of safeguards which need to be put in place. Nomination of point of contact, transparency and reporting were overall seen as non-problematic albeit some noted the need for flexibility.

For a more detailed overview of the content of the three options, these are presented in more detail in **Table 2** below.

**Table 2 Terrorism -specific legislative options: overview of alternative scenarios**

| Action | Option 1 | Option 2 | Option 3 |
|---|---|---|---|
| ***Scope of Application*** | | | |
| **Definition of terrorist content** | **Narrow definition**<br><br>material disseminated with purpose to directly incite a terrorist act produced by an EU listed terrorist organisations | **Comprehensive definition**<br><br>material disseminated with purpose to incite, recruit and train for terrorism, including in particular material produced by EU listed terrorist organisations | **Comprehensive definition**<br><br>material disseminated with purpose to incite, recruit and train for terrorism, including in particular material produced by EU listed terrorist organisations |
| **Material scope:** Hosting Service Providers | ✓ | ✓ | ✓ |
| **Geographic scope:** companies directing/offering services to EU citizens | ✓ | ✓ | ✓ |
| ***Removal of terrorist content*** | | | |
| **Action upon removal order** | Requirement to have measures, procedures and tools in place that enable the HSP to remove within 1h<br><br>Designation of competent authorities but no obligation to establish such entities<br><br>Feedback from companies on action taken | Requirement to have measures, procedures and tools in place that enable the HSP to remove within 1h<br><br>Designation of competent authorities but no obligation to establish such entities<br><br>Feedback from companies on action taken | Requirement to have measures, procedures and tools in place that enable the HSP to remove within 1h<br><br>MS to establish competent authorities with capacity to detect and notify terrorist content<br><br>Feedback from companies on action taken |

www.parlament.gv.at

| Action | Option 1 | Option 2 | Option 3 |
|---|---|---|---|
| **Action upon referrals** | | Requirement to have procedures in place to make an assessment on referrals from **Europol**<br><br>Such an obligation would be combined with more specific requirements to ensure the quality of referrals<br><br>Feedback from companies on action taken | Requirement to have procedures in place to make an assessment on referrals from **Europol and Member States.**<br><br>Such an obligation would be combined with more specific requirements to ensure the quality of referrals<br>Feedback from companies on action taken |
| **Proactive measures (applicable to companies exposed to terrorist content)** | Requirement to carry out a standardised risk assessment, in cooperation with Member States and where appropriate Europol.<br><br>Risk assessment would include (1) threat of terrorist activity, known intent and perceived attractiveness of the HSP (users/viewers, business model) (2) vulnerability (i.e. effectiveness of measures already in place) (3) identification of the level of risk.<br><br>Establishment of a remedial action plan is not mandatory but can be established with the involvement of the authorities. | Obligation to present a remedial action plan which should contain appropriate measures, proportionate to the level of risk and the specific circumstances of the company, to prevent the dissemination of terrorist content on their services.<br><br>Such measures **may include,** where appropriate automated means to detect, identify and expeditiously remove terrorist content **which has already been removed** following a removal order or referrals, as well as to immediately prevent content providers from re-submitting such content, in cooperation with competent authorities and Europol. | **Obligation** to identify and put in place measures, proportionate to the level of risk and the specific circumstances of the company to prevent the dissemination of terrorist content on their services.<br><br>Such measures **shall include,** where appropriate automated means to detect, identify and expeditiously remove terrorist content:<br>1) which has already been removed following a removal order or referrals, as well as to immediately prevent content providers from re-submitting such content and, as appropriate<br>2) reliable technical means, such as automatic detection technologies, to detect and **prevent the appearance of new terrorist content**, in cooperation with competent authorities and Europol. |
| ***Role of Europol and cooperation with law enforcement*** | | | |
| **Cooperation between national authorities (and** | Points of contact in HSPs for the purpose of | Points of contact in HSPs for the purpose of | Points of contact in HSPs for the purpose of |

www.parlament.gv.at

| Action | Option 1 | Option 2 | Option 3 |
|---|---|---|---|
| **HSPs) and Europol** | receiving legal orders | receiving legal orders and Europol referrals<br><br>Requirement for MS to inform, cooperate and coordinate with each other.<br><br>**MS may inform Europol of the removal orders and action taken by HSPs** | receiving legal orders and Europol referrals<br><br>Requirement for MS to inform, cooperate and coordinate with each other.<br><br>**MS may channel removal orders through Europol**<br><br>**HSPs may channel their feedback on removal orders through Europol** |
| **Requirement to maintain accessibility of terrorist content** for law enforcement purposes | **Reporting** obligation for HSPs on suspected criminal offences | **Reporting** obligation for HSPs on suspected criminal offences | **Retention** of terrorist content for law enforcement purposes<br>**Reporting** obligation for HSPs on suspected criminal offences |
| ***Safeguards, transparency and accountability*** | | | |
| **Due diligence requirements** for HSPs to avoid erroneous removal of legal content | ✓ | ✓ | ✓ |
| **Complaint procedures and judicial redress** for HSPs, content providers | ✓ | ✓ | ✓ |
| **Transparency reports** of HSPs | ✓ | ✓ | ✓ |
| **Reporting to the Commission** | Reporting requirements on implementation of the obligations, including information on proactive measures **taken voluntarily** by the company<br><br>Member States to report to the Commission on number of legal orders and referrals sent | Reporting requirements on the implementation of the obligations, including information on **proactive measures taken** by the company as part of the **remedial action plan**<br><br>Member States to report to the Commission on number of legal orders and referrals sent | Reporting requirements on the implementation of the obligations, including information on proactive measures by the company<br><br>Member States to report to the Commission on number of legal orders and referrals sent |

www.parlament.gv.at

| Action | Option 1 | Option 2 | Option 3 |
|---|---|---|---|
| ***Enforcement*** | | | |
| **Sanctions**<br>Member States to establish regimes under national law including designation of relevant authority<br><br>Determination of rules on jurisdiction | ✓ | ✓ | ✓ |
| **Requirement to establish a legal representative (for companies established outside the EU)** | ✓ | ✓ | ✓ |
| | | | |

www.parlament.gv.at

## 6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

All the retained options have been assessed against the following economic and societal impacts, in addition to other specific impacts on fundamental rights, presented in the next section. **Table 3** summarises the assessment. There are no significant environmental impacts to be assessed in the context of this initiative.

***Table 3 Screening and evaluation of impacts***

*( Symbols: + some positive impacts, ++ positive impacts, +++ very positive impacts; - some negative impacts, - - negative impacts, - - - substantive negative impacts. Symbols such as - / + point to the de evaluation of both positive and negative impacts along two criteria detailed in brackets for the respective categories)*

| **Impacts** | **Options** | | |
|---|---|---|---|
| | **1** | **2** | **3** |
| **Economic impacts** | | | |
| Functioning of the Internal Market | ++ | + + | + + |
| Impact on competition | - | - | - |
| Competitiveness and effect on SMEs *(costs / support)* | -/ + | - / + | - - / + |
| Technological development and the digital market *(costs / incentive)* | -/ + | -/ + | -/ + |
| Public authorities *(costs / effectiveness)* | - / + | -/+ | -/++ |
| **Social impacts** | | | |
| Crime, terrorism and security | + | ++ | +++ |
| Safety of Internet users | + | ++ | +++ |
| Governance and good administration | + | + | ++ |
| **Impacts on international relations and third countries** | | | |
| Third countries and trade relations | ≈ | ≈ | ≈ |
| **Impacts on fundamental rights** | | | |
| Respect for private and family life and Protection of personal data | - | -- | --- |
| Freedom of expression and information | ≈ | - | -- |
| Freedom to conduct a business | - | -- | --- |
| Right to life and dignity | + | + | ++ |

### 6.1. Economic impacts

#### *6.1.1. Functioning of the Internal Market and competition*

All options can be assessed as having a potential positive effect on the functioning of the Internal Market compared to the baseline. All options would limit further fragmentation of the Internal Market with regards to administrative procedures and obligations required from hosting service providers.



www.parlament.gv.at

This would increase legal certainty for hosting service providers and reduce operations costs when providing services cross-border. Combined with supporting measures, all options will aim to increase trust in the Internal Market and thus increase uptake digital services.

Concerning competition, options 2 and 3 present potential challenges in terms of unequal access to technology and resources related to content moderation and filtering approaches. Option 1 does not pose such challenges since it does not foresee mandatory proactive measures. Given the specific economic dynamics of multi-sided markets with strong network effects, options requiring proactive measures and content filtering technologies might reinforce the relative market power of the very large companies which have already internalised costs for the associated processes, or which have preferential arrangements between them to share specific technologies, if these technologies are not available to all market participants. This will be mitigated by the fact that proactive measures are required only from companies which are exposed to terrorist content, estimates pointing to an interval of 150 to 400 companies. Such measures should be proportionate to the risk and resources of the company. Option 2 would be less intrusive, allowing companies to choose the types of measures most appropriate in their specific case, whereas Option 3 would require them to put in place, where appropriate, automated tools for detection and removal of content.

In addition EU R&D&I actions to support the development of further technologies62 could eventually be shared and could support SMEs.

*6.1.2. Impacts on businesses and SMEs*

Almost 10.000 hosting service providers in Europe are small, medium, or micro enterprises63, about half of which are micro-enterprises. As larger platforms are increasingly hostile to terrorist content online, illegal content is increasingly disseminated via a diverse set of smaller platforms. Compared to around 30% in 2017, nearly 70% of Europol referrals in 2018 were sent to hosting service providers which can be considered small or micro enterprises. All options consider SMEs, including microenterprises, as part of the affected stakeholder group.

Some of the obligations in option 2 would imply a burden on companies, in particular for small and micro-enterprises, however these are mitigated by ensuring that measures are proportionate as well as reducing the number of companies who need to apply them to the ones exposed to terrorist content. Based on the number of service providers currently identified as hosting terrorist content, obligations relating to proactive measures and preservation of data would affect in principle between 150 to 400 companies, so between 1.5%-4% of the 10,000 hosting service providers mentioned above.

The main costs of options 1, 2 and 3 on businesses are estimated in Table 4 below and further explained in Annex 4. For all options, the major costs are those related to the application of the 1 hour deadline for removal orders. For option 1, this is likely to be slightly smaller than for 2 and 3, given the more restrictive definition given to the content which would result in a smaller number of orders. Other cost items are related to implementing content moderation or filtering technologies for companies exposed to terrorist content (under Option 3 and, up to the company's decision, under option 2 and, possibly option 1), as well as costs related to the risk assessment in option 1, remedial action plan in option 2 and providing feedback on actions taken as well as transparency and reporting

62 E.g. under Horizon 2020, Societal Challenge Secure Societies: Protecting freedom and security of Europe and its Citizens, the 2018-2020 Work Programme

63 Estimated number of SMEs with fast growth-potential,, based on the Dealroom database, *supra*, p. 6



www.parlament.gv.at

requirements. Since these obligations cover distinct functions and expertise, they will generally require dedicated staff or resources. Some of the costs are assumed to be absorbed in moderation functions already in place for other types of content.

In addition, the burden on SMEs would be further alleviated via funding into research and development of public tools made available at minimal cost to the companies. *Ad minima*, such tools would ensure better coordination across national authorities and limit duplication in treatment of referrals and removal orders, streamlining the companies' efforts to respond to national authorities. Such tools could evolve towards mutualisation of databases for filtering terrorist content previously identified through removal orders.

*Table 4 Estimate costs on hosting service providers (total costs compared to the baseline)*

| Option | Estimated costs |
|---|---|
| **1** | 1.0 – 5 FTEs + limited recurrent costs (see Annex) |
| **2** | 1.0 – 8.0 FTEs (+ cost of installing proactive measures; actual cost will depend on risk, resources and vulnerability of companies) + limited recurrent costs (see Annex) |
| **3** | 2 – 11.5 FTEs (+ cost of installing and maintaining internal and external filtering technology + marginal recurrent costs (see Annex) |

### *6.1.3. Technological development and the digital market*

Requirements under **all options** could divert internal company resources from innovation and growing the business towards ensuring compliance (as regards responses to removal orders, referrals, complaint procedures and transparency requirements and, in particular, proactive measures, including costs for staff and development and/or deployment of automated tools). At the same time, they can also be expected to incentivise further specific technology development to remove terrorist content online. Some EU companies64 have begun to develop automatic content detection, filtering and moderation technologies, and this sector will potentially see increased growth as companies look for technologies to facilitate compliance.

On a more general level, to the extent that all **options** incentivise companies to establish more robust mechanisms against illegal content online, this will have a positive effect on trust into their services and in the Digital Single Market which can lead to greater uptake of digital services, which would attract more investment, attract uses, and increased advertisement revenues although these benefits are difficult to quantify. In addition, the options will be combined with supporting measures to further mitigate some of the costs on companies and support technological development and the development of new innovative approaches to tackling an evolving problem.

### *6.1.4. Administrative burden and costs for public authorities*

Under all the options, the overall impact related to the costs of introducing a removal order is expected to be neutral for public authorities, since in option 1 and especially in option 2 (given the comprehensive definition) the resources currently used for referrals would cover also removal orders. The increased legal clarity would lead to better removal rates; efficiency gains are likely to be particularly evident for removal orders addressed to currently non-cooperative companies. Option 1

64 E.g. ASI Technologies, or besedo.com as some examples



www.parlament.gv.at

would involve minimal additional costs for Member States to the extent that they would have to participate in companies' risk assessments. However, option 2 and, to an even larger extent option 3, would alleviate public authorities from certain costs to the extent that increased deployment of proactive measures should reduce the necessity for removal orders or referrals. Option 3 would nevertheless imply significant costs for Member States which do not yet have adequate capabilities to detect and notify illegal content online to establish them. Under options 1 and 3 costs ranging from moderate to significant could also be expected for Member States, depending on their procedures related to content reported by companies on suspected criminal offences. Costs of this particular measure are difficult to quantify given that the amount of content is unknown and subsequent follow up actions vary from one Member State to another.

The table below summarises these impacts:

| **Who bears the cost** | **Option 1** | **Option 2** | **Option 3** |
|---|---|---|---|
| **National public authorities** | Cost of establishing sanctions, reporting monitoring 0.5 FTE + 0,5 x 5 FTE to assist with risk assessment | Cost of establishing sanctions, reporting monitoring 0.5 FTE + 0,5 x 5 FTE for enhanced cooperation to reinforce effectiveness of measures | Cost of establishing sanctions, reporting monitoring 0.5 FTE + Average of 3-4FTE to establish detection capacity in 23 MS + costs related to content received from companies |
| **EU-level (including Europol)** | 1 FTE for assistance with risk assessment | 1 FTE for enhanced cooperation to reinforce effectiveness of measures | 3FTE for enhanced cooperation to reinforce effectiveness of measures |

## 6.2. Social impacts

The social impacts of the different options are assessed in relation to their effect in terms of disrupting the capacity to spread illegal content on the Internet, as well as of the underlying illegal activities, both online and offline, and increasing the capacity of public authorities to combat crime. Impacts on the safety of Internet users and more generally the victims of illegal activities (both online and offline) have also to be assessed. Finally, in an increasingly digital society, the measures considered would also have some impact on governance and good administration considered as a whole.

### *6.2.1. Crime, terrorism and security*

All options would have a significantly positive impact on security, since it would help reduce in a comprehensive and effective manner the dissemination of terrorist material online. All three options would ensure that service providers from within and outside the EU apply actions to prevent the presence of terrorist content on their platforms, in particular companies that are exposed to being misused for terrorist purposes. The greater the requirements on companies as regards reactive and proactive measures, the greater the positive impact on security: options 2 and 3 would thus have a significantly greater effect than 1, given that option 1 has a narrow definition and does not include obligations for proactive measures.



www.parlament.gv.at

In addition, all options would reinforce the ability of competent national authorities and Europol to combat terrorist content online, notably by increasing the speed of response by companies to removal orders and the speed of assessment of referrals, and to combat terrorist activities more generally. This is reinforced by the obligation in all options to report cases which the hosting service provider considers would constitute a terrorist offence or result in a threat to life or safety of people. In addition, in option 3 companies would be required to retain for a period of time the content they have removed either proactively or in response to referrals, further enabling law enforcement to have access to information which can be crucial for investigations, analysis or for evidence purposes.

*6.2.2. Safety of Internet users*

**All options** would seek to improve the safety of users of online services with a view to protecting them from harmful content online, and limit the access to terrorist materials for individuals vulnerable to terrorist radicalisation. Provisions related to reporting the content alleged terrorist content to authorities in all options would contribute to enabling them to better ensure the safety of citizens.

Option 3 would deliver the greatest impact in terms of reducing the most amount of terrorist material, as those HSPs affected would be obliged to put in place measures, including where appropriate automated detection to identify all terrorist content including new content or to prevent the re-uploading of terrorist content. This would ensure higher volumes of removal of terrorist content than option 1. Furthermore, there is a question as to whether without a requirement for automated means, users would see much of a reduction under option 1, particularly given the narrow definition. Option 2 is more similar to option 3 in that it places a duty on hosting services to take appropriate and proportionate action, leaving the means and the tools to their discretion. This would therefore ensure higher volumes of terrorist content would be removed than option 1, but less than option 3. In conclusion, option 3 would deliver the most impact in terms of reducing the volume of terrorist content accessible to users.

*6.2.3. Governance and good administration*

All options would add clarity as to the role of administrative and law enforcement authorities of Member States in dealing with terrorist content hosted by service providers, by providing a clear definition and a legal framework for dealing with the detection, identification and removal of terrorist content and by providing also for the necessary safeguards to ensure the full respect of fundamental rights. All options would contribute positively to transparency and public governance through transparency requirements and feedback mechanisms of removal orders. Option 2 would provide further clarity on obligations with regards to Europol referrals and option 3 would harmonise the approach even more so as it would also include Member State referrals. Requirements for Member States to coordinate and cooperate their actions under options 2 and 3 ensures efficient allocation of resources by avoiding duplication of removal orders and referrals while avoiding interferences with ongoing investigations.

### 6.3. Impacts on third countries and international relations

The three main options examined have a similar geographic scope, targeting service providers established both within, and outside the EU insofar as they offer service within the Union. All those companies would need to appoint a legal representative to be able to receive removal orders from Member States. Since the same obligations would apply world-wide, as long as companies offer services to European users, no additional barriers to trade or distortions would be created. As a knock-



www.parlament.gv.at

on effect, more effective measures taken against illegal content in the EU, would lead to less illegal content available in third countries, given the global nature of the Internet.

As regards terrorist content online, major trading partners, e.g. in the G7 and G20 group of nations, have called on Internet companies to step up their efforts against terrorist content online, although some are likely to be concerned about the imposition of EU rules on companies established in their jurisdiction. On the other hand, all nations concerned about terrorism online would benefit from EU rules even if their companies would see themselves exposed to EU regulatory burdens and compliance costs. However, should a conflict of law situation arise, the hosting service can disable access to the content within the EU.

### 6.4. Impacts on fundamental rights

Each of the options may have both a beneficial and a negative impact on fundamental rights, as they do not impact equally in each of the rights. Service providers' freedom to conduct business can be subject to interference by the proposed measures, as well as users' freedom of expression and information, right to personal data protection or right to respect for private and family life could negatively be affected, at different levels, depending on the proposed measures. However, some of the policy options, including the obligation for hosting service providers to inform law enforcement of terrorist content that could pose a threat to life and safety could have a positive impact on the right to life.

***Table 5*** *Impacts on fundamental rights: summary. Symbols: + some positive impacts, ++ positive impacts, +++ very positive impacts; - some negative impacts, - - negative impacts, - - - substantive negative impacts.*

| Fundamental right – Article | | Option 1 | Option 2 | Option 3 |
|---|---|---|---|---|
| 7 | Respect for private and family life and Protection of personal data | - | -- | --- |
| 11 | Freedom of expression and information | ≈ | - | -- |
| 16 | Freedom to conduct a business | - | -- | --- |
| 1/2 | Right to life and dignity | ≈ | + | ++ |

**Option 1** has limited negative impact on freedom to conduct a business, as it introduces binding obligations to take action after receiving a removal order within one hour, but leaves companies their freedom to take further measures in relation to narrowly defined terrorist content (only material inciting the commission of terrorist acts). As regards freedom of expression and information (to the extent that removed material can be regarded as being protected under Article 11 of the Charter) the impact would also be limited since there would be no requirement to establish proactive measures.

**Option 2** is considered to have a more negative impact on freedom to conduct business, as stricter obligations would be imposed to the hosting services providers. However, the specific choice of the set of measures would be left to the discretion of the provider, based on the proportionality and necessity as regards the assessed risk and to the company's resources.

There are also risks to negatively affect the right to freedom of expression linked to the obligation to establish automatic tools aimed at preventing the re-upload of content previously identified as terrorist content, to the extent that erroneous detection could lead to removal of legal content protected under Article 11 of the Charter. The deployment of automated tools to filter previously identified content cannot account for contextual interpretation of the legal use of the content (e.g. for journalistic



www.parlament.gv.at

purposes, archiving for research purposes). As such, any tools would need to be accompanied by safeguards, including where appropriate, human review. Even so, the use of the technology may accidentally lead to removal of legal content, this should be mitigated by informing the content uploader of the removal, and the accessibility of effective complaint mechanisms.

The rights to personal data protection and privacy are also negatively impacted as far as this policy option may involve further processing of personal data than Option 1, not only where referrals are received from Europol, but also where proactive measures are taken, including by means of automated means to detect, identify and remove terrorist content, as well as to prevent such content from being re-submitted.

The impact on the right to life and dignity could be positive compared to the baseline and in option 1, given that the measures put in place would be more effective and result in larger number of harmful content being removed potentially preventing terrorist propaganda from translating into to action. Moreover, the obligation to report incidents of suspected terrorist offences where there is threat to life or safety of people would ensure that cases of imminent threat are communicated to the national authorities.

Compared to Option 2, **Option 3** imposes an additional obligation to host services providers exposed to terrorist content to use reliable tools to automatically identify terrorist content, including by preventing re-upload and by detecting new content not previously identified by a competent authority. Such technologies are more costly than those included in option 2, they depend on access to high quality data on which it can be trained and require human reviewers both during development and deployment.

Moreover, while the detection technology is improving, it is still prone to errors, particularly when linked to language detection and when it requires contextual understanding of the content, and presents risks of erroneous removal of legal content thus presenting a potential negative impact to the right to freedom of expression and information.

The impact on data protection and privacy is also higher than in Option 2, not only because enhanced obligations on hosting service providers in case of referrals and proactive measures involve more data processing, but also because this Option would entail preservation of data, for the purpose of reinstating the content in cases of erroneous removal as well as for law enforcement purposes.

At the same time, Option 3 would have the most positive impact on the right to life and dignity as in addition to all the measures under option 2, it would result in more harmful content being removed and would reinforce competent authorities' investigations and strengthen their capacity to combat terrorist activities.

**Safeguards mitigating negative impacts**

The potential negative impacts of the policy options, and in particular, the interference of a potential obligation to establish automated detection tools on freedom of expression, have been raised as a concern by several groups of stakeholders, including contributions from citizens in the public consultation, as well as academics, civil society representing digital rights, as well as companies.

In order to address these risks and concerns, it is necessary to accompany any future instruments with robust safeguards that minimise the risk to excessively and disproportionately interfere with the provider's freedom to conduct their business as well as potential erroneous removal of legal content.



www.parlament.gv.at

The first safeguard to protect freedom of expression would be that any instrument as result of the different policy option would be clearly rooted and linked to the definition of terrorist offences in Directive (EU) 2017/541which would limit the instances of removals  legal content. This definition would apply to removal orders and referrals, as well as to proactive measures. The link to the definition of terrorist content under EU law would ensure that the content removed is not be protected under Article 11 of the Charter as largely established by the relevant case law of the European Court of Human Rights.

Regarding removal orders, the main responsibility of assessing the content and ordering the removal stays with the competent authority, which would have to undertake a thorough check of the content and be subject to legal controls before the issuing of the order justifying the one hour removal time for this measure. The risk of erroneous removal of legal content in this scenario is therefore particularly low and judicial redress would be available to challenge any removal order issued.

For referrals, the responsibility for removing content rest with the hosting service providers. This means that they need to assess the content before taking action but this assessment facilitated by the prior appraisal of EU (Europol) and national authorities with particular expertise to identify whether or not the content could potentially constitute terrorist content as defined by law. This safeguard together with the right for the content provider to issue a complaint to challenge the removal of the content in question would limit the number of cases where the content identified is erroneously removed.

For proactive measures, the responsibility for identifying, assessing and removing stays with the hosting service providers. In this scenario substantial safeguards are needed to limit the negative impact to freedom of expression. First for proactive measures consisting in detecting and removing re-uploaded terrorist content, the risk would be substantially decreased by ensuring that the  measures only target content previously identified by a competent authority as terrorist content as well as provide for human review if further contextualisation is required.

For proactive measures aimed at detecting new terrorist content, companies would be obliged to establish safeguards to prevent removal of legal content, and in particular, would be encouraged to include human review when deploying such technology. Furthermore, unlike in the baseline scenario where the most affected companies set up automated tools without public oversight, the design of the measures as well as their implementation would be subject to reporting to competent bodies in Member States. The obligation to provide information on the functioning of the safeguards reduces the risks of erroneous removals, both for companies setting up new tools as well as for those who are already using them.

In this respect, it is important to note that public oversight would also concern the accuracy of tools to detect new content. Reporting obligations would allow public authorities to scrutinize the functioning of automated detection. In this context, it is also important to distinguish between automated detection and automated removal. The policy options propose automated detection, acknowledging the need for human oversight and verification before removal.

Finally, in each option the obligation to establish proactive measures is proportionate to the risk of hosting terrorist content as well as economic capacity of the provider, thus ensuring that only those companies effectively at risk have an obligation to establish proactive measures and that the measures adopted contain a set of safeguards. As such the policy options ensure the protection of freedom of expression and .  also provide safeguards to respect the right to conduct a business.



www.parlament.gv.at

In addition to these measures, an important safeguard are the possibilities for the users whose content was removed to contest the removal decision. Judicial redress would be available for both service providers and content providers to appeal removal orders issued by a national authority. For content removed by a decision of the hosting service provider, companies would have a general obligation to inform the users when their content is removed and put in place user-friendly complaint mechanisms in cases of erroneous removal. If these remedies would conclude that a removal was not justified, the requirement to preserve removed material as foreseen in option 3 would allow the reinstatement of the content.

These specific safeguards would be accompanied by a general requirement of transparency towards the public regarding companies' actions. The requirement to make publicly available their overall policy with regards to terrorist content and to publish regularly transparency reports with precise data on removal, complaints and reinstatement of content, should incentivise companies as well to apply a high level of accuracy before deciding on removing content.

From a data protection perspective, the general data protection rules will be applicable. However, in order to ensure that the interference with the right to the protection of personal is limited to what is strictly necessary, it is essential that any future instrument lays down clear and precise rules governing the scope and application of measures involving processing of personal data and imposes minimum safeguards so that the persons whose data have been processed – especially in cases of retention for law enforcement purposes – have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data. Specific safeguards should include a transparency obligation regarding the data processing undertaken by hosting service providers, an obligation to inform the concerned persons where their content is taken down, a specific complaint mechanism, a specific obligation of human oversight and verification on automated individual decision-making and, when it comes to data retention for law enforcement purposes, a limited period of retention and measures to ensure that targeted data is protected against any unlawful access and use.

**Stakeholders' views**

The general public, both in the Eurobarometer and the open public consultation, the overwhelming majority (over 85%) agreed that freedom of expression needs to be protected. In the Eurobarometer, 75% of the respondents considered that the user should be able to appeal the decision when the Internet hosting service removes content uploaded by a user.

In the open public consultation, the civil society organisations, despite having issues with the current framework, especially in terms of transparency of the processes for removing illegal content or contesting a removal, expressed a concern about the impact proactive measures or new legislative measures may have on freedom of expression and information. This specific point was also pointed by academics who flagged the need for a thorough understanding of the incentives for over-removal, which can be set in place by legislation requesting intermediaries to intervene too fast and through proactive, automated tools.

They were concerned that decisions by platforms about controversial content according to their terms of service in a non-transparent way may impact the rule of law and ultimately endanger freedom of expression. Thus, they agree with reinforcing public authorities' capabilities in fighting illegal content on-line and are not particularly in favour of attaching privileges to trusted flaggers or imposing on platforms an obligation to report to law enforcement bodies all alleged illegal content. Like respondents in other groups, they are not keen on out-of-court dispute resolution procedures either.

Respondents to the Eurobarometer considered that Internet hosting services should process all notifications they receive and assess the legality of the content (86%) and that hosting services should immediately remove content flagged as illegal by competent authorities and law enforcement bodies (90%). Additionally, 85% of respondents considered that Internet hosting services should immediately remove content flagged as illegal by organisations with proven expertise on the topic. In the



www.parlament.gv.at

open public consultation, nearly half of the respondents considered that hosting services should remove immediately content notified by law enforcement authorities, whereas 25% opposed such fast-processing. Half of the respondents opposed fast removal for content flagged by organisations with expertise (trusted flaggers), other than law enforcement, but 25% agreed with such fast procedures.

Most of the Member States that responded to a targeted survey also expressed a concern over possible erroneous removals of legal content and suggested a range of possible safeguards and mitigating measures, inter alia: temporary removals before assessment takes place, independent oversight, human-in-the-loop for automation, or appeal procedures as well as prior legality assessment by competent authorities in case of imposing 1-hour removal.

Companies consulted as part of a targeted questionnaire on terrorist content also noted the need to address concerns of erroneous removals, especially with tight timeframes, while noting that safeguards are also resource intensive. As such, measures should be proportionate to the size of the service provider.

## 7. HOW DO THE OPTIONS COMPARE?

In the comparison of options, the following criteria were used:

- **Effectiveness,** covering
  - Limiting legal fragmentation and facilitating cross-border service provision (objective 1)
  - effectiveness of measures to detect, identify and remove illegal content, specifically terrorist content (objective 2);
  - increasing transparency and accountability of platforms for measures taken to detect, identify and remove terrorist content (objective 3);
  - improving the ability of relevant authorities to intervene against terrorist content online and to combat crime (objective 4) and
  - providing safeguards against the risk of erroneous removal of legal content and ensure protection of fundamental rights (objective 5).
- **Efficiency** ratio between the costs incurred, and the benefits expected in pursuing the above-mentioned policy objectives.
- **Coherence** with (a) DSM policy supporting platform innovation, (b) coherence with the acquis framing applicable in the DSM, (c) coherence with Internet principles and the technical infrastructure of the internet65; (d) Terrorism Directive.
- **Proportionality**: as the ratio between the effectiveness of the policy option in reaching the policy objectives and its efficiency and impact on fundamental rights (considering only potential negative impacts)

***Table 6 Comparison of options***

| **Option** | **Effectiveness** against objectives: | | | | | **Efficiency** (cost/benefit) | **Coherence** against policies: | | | | **Proportionality** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | | a | b | c | d | |
| Baseline | ≈ | ≈ | ≈ | ≈ | ≈ | ≈ | ≈ | ≈ | ≈ | ≈ | ≈ |

65 Screening against Tool 27 in the Better Regulation toolbox, and the Commission's policy on Internet Governance (COM (2014) 072 final)



www.parlament.gv.at

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Option 1 | + | + | ++ | + | ≈ | -/+ | - | + | --- | + | + |
| Option 2 | ++ | ++ | ++ | ++ | ≈ | --/++ | - | + | --- | + | + |
| Option 3 | ++ | +++ | ++ | +++ | ≈ | ---/+++ | - | + | --- | + | + |

## 7.1. Effectiveness

*Objective 1: Facilitate the provision of online services across the Digital Single Market by limiting further legal fragmentation*

All options will contribute to the provision of online service across the digital single market as they will limit the emerging legal fragmentation on Member State level and will provide a harmonised definition of terrorist content online. The difference between the options relates to the scope of the definition which is limited to content which incites to terrorism under Option 1. Options 2 and 3 adopt a broader approach, in addition to incitement, they also include material which relates to recruitment and training. The latter may lead to greater legal certainty as it is more likely to discourage Member States to issue removal orders under national law.

*Objective 2: Increase the effectiveness of measures to detect, identify and remove terrorist content*

All options would be significantly more effective than the baseline scenario insofar they would establish clear obligations applicable to all hosting service providers (also beyond those established in the EU) to act against terrorist content against a clear definition subject to sanctions in case of non-compliance.

Due to their design, options are incrementally more effective (2 more than 1 and 3 more than 2) as regards companies' actions, since the requirements for reactive as well as proactive measures would be more stringent and wider in each option. The effectiveness of option 1 would mainly relate to the impact of the measures on removal orders, which would be positive as compared to the baseline. At the same time, options 2 and 3 would be more effective in this respect since the more comprehensive definition of terrorist content would allow for significantly more removal orders and since the options include referrals.

The effectiveness of proactive measures would be limited in option 1 to the companies that would voluntarily put them in place following the risk assessment. The requirements to take proactive measures in option 2 would be limited to preventing the re-upload of already identified content via a removal order or a referral and as such, the most effective measures to improve and detect terrorist content would be under option 3 which also includes the detection of new content. The deployment of proactive measures have equalled to substantial increases and more effective removals of terrorist content, where in general, referrals only account for a small proportion of the total content removed66. Depending on companies, the rate of terrorist content removed on the basis of proactive measures varies across companies, reaching up to 99% for some companies.

*Objective 3: Increase transparency and accountability of platforms for measures taken to detect, identify and remove terrorist content*

66 See section 2.3.2 "Illegal Terrorist content is accessible online, reappears, and spreads across service providers posing a security challenge" as well as Annex 8 and 9.



www.parlament.gv.at

All options would significantly increase accountability in view of the scope of companies covered, since all companies exposed to terrorist content would have to develop and publish transparency reports. A substantially higher number of companies would publish these reports than in the baseline scenario, although the transparency requirement would apply specifically to actions and safeguards on terrorism content. It is also likely that many companies would also publish data for other types of content.

In terms of accountability towards public authorities, the same logic applies: a considerably higher number of service providers would report more detailed information about their actions against terrorism content than it is the case today. This would include clear data about actions taken upon receiving removal orders and referrals, and in options 2 and 3, on the proactive measures taken by the company and the safeguards in place.

*Objective 4: Improve the ability of relevant authorities to intervene against terrorist content online and combat crime*

All options are likely to have a positive effect on the ability of relevant authorities to intervene against illegal content online. In option 1, the positive effect mostly relates to the expected increased response rated to removal orders. In option 2, in addition to removal orders, the obligation on hosting service providers to report removed content to law enforcement related to suspected criminal offences and to provide feedback on Europol referrals would further increase the ability of relevant authorities to intervene. Option 3 would be most effective in this regard than options 1 and 2 as it would include, in addition, feedback on Member State referrals and preservation of removed content by hosting service providers.

*Objective 5: Safeguard against the risk of erroneous removal of legal content and ensure protection of fundamental rights*

A number of measures common to all options would mitigate the risks on fundamental rights. Notably, a clear definition of what constitutes terrorist content online will assist assessment and provide legal certainty. Requirement to inform content providers and set up easily accessible complaint mechanisms as well as obligatory transparency will improve safeguards vis-à-vis users. In addition, the design and implementation of proactive measures including automated detection would be subject to scrutiny by competent authorities which is a considerable improvement compared to the baseline.

## 7.2. Efficiency

The efficiency assessment of the options follows a qualitative cost-benefit analysis described with more details in Annex 3. While the options come at varying costs in particular for hosting service providers, their benefits are also proportionate: i.e. higher the costs, more important the benefits. Overall, all the options can be considered efficient insofar as the costs incurred under each option are balanced as to the benefits to be expected in reducing terrorist content online to increase trust in the digital single market and enhance security. The non-negligible compliance cost will be somewhat mitigated by flanking measures to further develop technologies, as well as by streamlining coordination processes across competent authorities, limiting the costs for hosting service providers in dealing with multiple authorities.

Under **option 1** there would be higher costs for hosting providers for compliance compared to the baseline, but overall they would benefit from a more secure online environment and increased trust in



www.parlament.gv.at

online services. However these benefits are limited by the narrow definition as to the content to be removed, limiting the effectiveness of companies' actions and put the focus on reactive measures, which are less effective than proactive measures in reducing illegal content online as required in options 2 and 3.

For **option 2**, there will be higher costs for hosting providers than in option 1, but obligations for measures to be taken would be adapted to the size and business model of the company, where appropriate. Overall significant benefits are expected as regards the reduction of terrorist content online, since there would be a higher number of terrorist content removed due to the more effective response to takedown content identified by national authorities (and, in contrast to option 1, by Europol) as well as the establishment of proactive measures. Furthermore, thanks to these actions, companies would benefit from a more secure online environment and increasing trust in online services.

Under **option 3** some hosting service providers will experience an increase in costs compared to options 1 and 2 given that companies exposed to terrorist content would need to take more far reaching proactive measures. Under this option a higher cost is also foreseen for Member States to the extent they would be required to establish dedicated entities tasked with the detection, identification and notification of terrorist content to hosting service providers. Overall more benefits are expected in establishing a more secure online environment compared to 1 and 2.

## 7.3. Coherence

| **DSM policy supporting platform innovation** |
|---|
| • All legislative options entail a considerable compliance cost on hosting service providers, potentially burdensome on start-ups. In the design of the options, this is mitigated as the proactive measures are foreseen proportionate to the risk and economic capacity of the HSP. In addition, the prevention of further legal fragmentation prevents even more burdensome costs on HSPs offering their services cross-border. |
| **The DSM acquis, in particular the E-Commerce Directive** |
| • To the extent that the proactive measures required under each of the options are only limited to companies exposed to terrorist content, are necessary and proportionate in particular taking into account the level of exposure to terrorist content and economic resources of the service provider, and they amount to specific monitoring obligations, all options are designed to be compliant with the E-Commerce Directive and in particular Article 15 (1). |
| **Coherence with internet principles and the technical infrastructure of the internet67;** |
| • All policy options are generally coherent with the technical infrastructure of the Internet; when certain proactive measures are used by hosting services, these may entail some alterations to the effective functioning, in particular when upload filters are deployed. |
| **Terrorism Directive** |
| • All policy options are coherent with the Directive (requiring Member States to take action to ensure the swift removal of certain types of terrorist content) reinforcing the legal framework by establishing clear obligations directly on companies with a focus on preventing the dissemination of terrorist material in the necessary broad sense and ensuring effective removal or disabling of access across Europe. |

67 Screening against Tool 27 in the Better Regulation toolbox, and the Commission's policy on Internet Governance (COM (2014) 072 final)



www.parlament.gv.at

## 7.4. Proportionality

Against a dynamic baseline, the added value of the different options as well as the proportionality of the intervention depends on the balancing between the need for effective measures to detect, identify and remove terrorist content online, the burden and responsibility placed on hosting service providers as well as the potential negative effects on fundamental rights of third parties.

The comparison of options shows that all legislative options imply costs which are not negligible, in particular for hosting service providers. These costs are higher under option 3 to the extent that companies will be obliged to take more far reaching proactive measures. Likewise, costs for Member State are higher under option 3 to the extent that they would need to ensure that relevant authorities have sufficient capabilities to detect, identify and request removal of terrorist content.

On the other hand, and while coming at a higher cost, proactive measures enhance the effectiveness of measures to detect, identify and swiftly remove terrorist content online and thereby increase the trust in the online environment as well as overall security for hosting service providers, users and the society in general, with the variations explained above.

The different options overcome legal fragmentation (in particular as regards procedures requesting hosting service providers to remove terrorist content) and increase legal certainty regarding hosting service providers' responsibilities (including in particular through a definition of illegal terrorist content and clarification of duties of care), with certain variations depending on the option. At the same time, the different options impact fundamental rights of hosting service providers and users in different degrees, with option 3 requiring more far reaching proactive measures having a potentially higher negative impact. However, adverse effects on the fundamental right to freedom of expression and information are mitigated through strong safeguards including judicial redress and complaint procedures but also requirements of transparency and due diligence for instance as regards human oversight and verification of content surfaced through automated detection tools.

## 8. PREFERRED OPTION

The report has analysed a series of problems and risks and has proposed a number of options, each addressing the issues identified with different levels of requirements and balanced with appropriate safeguards, in particular as regards the protection of fundamental rights, with a view to limit the measures to what is effective, appropriate and proportionate.

Taking into account the particular need and urgency to prevent the dissemination of terrorist content online, there is a corresponding need to put in place measures which capture the most harmful content and are particularly effective while providing sufficient safeguards against undue interferences with fundamental rights.

A definition of terrorist content which captures the most harmful material in terms of radicalisation, recruitment, training, instruction and incitement to carry out terrorist attacks closely linked to the terrorist offences laid down in the Terrorism Directive (option 2 and 3) would therefore be preferable to a narrow definition of content (Option 1).

In terms of measures to prevent the dissemination of terrorist content online, proactive measures have proven to be particularly effective justifying the establishment of corresponding obligations on hosting service providers. The scope of obligations should be commensurate to the risk and level of



www.parlament.gv.at

exposure to terrorist content on the hosting services, as well as the economic capacity of the hosting service providers, where appropriate. Where necessary obligations should therefore not be merely limited to preventing the re-upload of already identified terrorist material but also the detection and removal of previously unknown or undetected material (as foreseen under option 3).

Requirements for proactive measures usefully complement the requests from public authorities to take down terrorist content. Setting out requirements in terms of prior assessment by the competent authorities facilitates the follow up action to be taken by hosting service providers and justifies particularly strict deadlines for removal orders.

Referrals have proven to be an effective means of increasing the hosting service providers' awareness of terrorist content enabling them to take swift action. The legislative initiative should therefore include provisions to ensure maximum impact and avoidance of parallel referral mechanisms used by Member States, the legislative proposal should cover both Europol and Member States referrals (as foreseen under option 3).

To ensure accuracy and effectiveness of removal orders and referrals, Member States should make sure that the competent authorities have the necessary resources and capabilities (as foreseen under option 3). To further streamline processes, ensure coordination and avoid duplication Member States would be obliged to inform, coordinate and cooperate with each other with regard to in particular removal orders (but also referrals). Member States could furthermore channel removal orders and referrals via Europol, allowing hosting service providers to channel also feedback via Europol on these referrals and removal orders.

Requirements related to the removal of terrorist content must be coupled with strong safeguards at different levels including due diligence to prevent erroneous removal of legal content, when hosting service providers use proactive measures, effective complaint and redress mechanisms, as well as transparency and reporting requirements to ensure that there are no undue interferences in particular with the freedom of expression and information. Reporting obligations would furthermore allow for monitoring of impact of the initiative.

As regards the economic impact of the envisaged requirements on in particular small or micro companies, account must be taken of the fact that it is smaller hosting service providers are increasingly used for hosting terrorist content. An exemption for such companies would therefore not be appropriate. However, for instance when determining the scope of obligations to take proactive measures, the risk and level of exposure to terrorist content as well as the economic capacity of the hosting service provider in question will be taken into account, ensuring proportionality.

**Based on this assessment of the measures proposed, policy option 3 is the preferred option.**

The most important feature of policy option 3 is the effectiveness of the measures to remove terrorist content online. The policy option would significantly contribute to achieving the policy objectives, the combination of the proposed measures brings most benefit in relation to the scale and scope of the problem. While the third option is expected to have the highest economic impact in relation to expected costs and additional administrative burden, it would also bring the highest benefits.

Given the potential negative impact on the right to privacy, freedom of expression and information and the right to conduct business a number of safeguards are foreseen to mitigate this. In addition, the policy option would have the most positive impact on the right to life and dignity, by surfacing terrorist content and supporting the intervention of law enforcement.



www.parlament.gv.at

## 9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

In line with activities already undertaken, the Commission will monitor, by funding relevant research actions and drawing on expertise from Europol, the behavioural patterns of terrorists' modus operandi online, as well as the technologies used for this purpose, and the impact of actions by hosting service providers. In addition, the Commission will monitor developments, and the performance of technological tools which can bring promising results in countering illegal content online.

Further assessment of the situation will be provided by INTCEN, as part of its work with security and intelligence partners within Member States, and, in parallel, by the EU Internet Referral Unit which will provide regular analysis for law enforcement partners. Regular transparency reporting by the companies will also provide detail on the level of industry action.

In order to ensure an effective implementation of the measures foreseen and monitor their results, the Commission will work closely with relevant authorities in Member States, EU agencies and institutions (especially Europol and EU INTCEN) and the hosting service providers.

Regular exchanges such as under the EU Internet Forum would allow to not only monitor developments but also to share experiences on the implementation of the legislation and other industry action in particular with a view to support smaller companies.

The monitoring will be based primarily on reporting from Member States complementing publicly available transparency reports. Some of this information will be gathered by the competent authorities during the course of their duties, such as data on removal orders and referrals. Other data, in particular on proactive measures, but also on issues such as complaint procedures, will be provided by hosting service providers as part of their reporting obligations.

Furthermore, and in line with better regulation rules, the evaluation of success/impact of the initiative will be based on a detailed programme for monitoring the outputs, results and impacts. The monitoring programme shall set out the indicators and means by which and the intervals at which the data and other necessary evidence will be collected. It shall specify the action to be taken by the Commission and by the Member States in collecting and analysing the data and other evidence to monitor progress and evaluate the legislation. Where need be, targeted surveys may be carried out to collect further information.

The table below summarises tentative indicators (subject to further refinement as part of the envisaged monitoring programme) proposed to monitor the achievement of specific objectives as well as the operational objectives linked to the various building blocks of the options.

| SPECIFIC OBJECTIVES | OPERATIONAL OBJECTIVES | INDICATORS | COLLECTION STRATEGY |
|---|---|---|---|
| Improve the ability of relevant authorities to counter terrorist content online | Increase capacity of MS authorities in detecting, identifying and requesting removals | Number of Member States issuing removal orders or sending referrals, follow-up action (including redress, sanctions) | Data reported to the Commission by Member State authorities |
| | Increase accountability of hosting service providers towards Member States | Number of companies reporting | Reporting by hosting service providers to Member States |



www.parlament.gv.at

| | | | |
|---|---|---|---|
| Effectiveness of measures to tackle terrorist content | Ensure a takedown of terrorist content notified to companies via removal orders within 1 h | Number of removal orders and rate of removals within 1h | Reporting by Member States (on the basis of own data and feedback by hosting service providers) |
| | Ensure high level of responsiveness to referrals (removals and feedback) | Number of referrals, removal rates, average time for feedback and removal | Reporting by Member States and Europol (on the basis of own data and feedback by hosting service providers) |
| | Promote companies implementation of proactive measures to detect, identify and remove terrorist content online | Number of companies putting proactive measures in place | Reporting by hosting service providers to Member States |
| | | Rate and speed of terrorist content online removed by hosting service providers' own tools | |
| | | Reliability of detection tools | |
| | Enhance coordination amongst Member States and Europol | Number of MS connected to Europol for channelling removal orders and referrals | MS and Europol data |
| Increase transparency and accountability | Improve awareness by users and citizens on companies policies against terrorist content online and safeguards | Number of companies publishing transparency reports | Reporting by hosting service providers to Member States |
| Safeguards against erroneous removal | Ensuring high level of accuracy of removal orders | Number of removal orders appealed | Member States data |
| | minimising the number of erroneous removals based on proactive measures | Number of complaints filed | Reporting by hosting service providers to Member States |
| | | Percentage of successful complaints | |



www.parlament.gv.at

Annexes





www.parlament.gv.at

# Annex 1: Procedural information

### LEAD DG, DECIDE PLANNING/CWP REFERENCES

This Staff Working Paper was prepared by the Directorate-General for Communications Networks, Content and Technology and the Directorate General for Migration and Home Affairs.

The *Decide* reference of this initiative is PLAN/2017/1766.

### ORGANISATION AND TIMING

The Impact Assessment was prepared by the two co-lead Directorates-General, in close collaboration with the Directorate-General for Justice and Consumers, as well as the Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs.

The Inter-Service Steering Group established for the work streams on online platforms was associated and consulted in the process, under the coordination of the Secretariat-General, including the following services: DG COMP (DG Competition), DG GROW (DG Internal Market, Industry, Entrepreneurship and SME), DG ECFIN (DG Economic and Financial Affairs), DG EMPL (DG Employment, Social Affairs and Inclusion), DG JUST (DG Justice and Consumers), DG TRADE, DG ENV (DG Environment), DG ENER (DG Energy), SJ (Legal Service)LS, EPSC (European Political Strategy Centre), JRC (Joint Research Centre), DG RTD (DG Research and Innovation), DG EAC (DG Education, Youth, Sports and Culture).

The last meeting of the ISSG, chaifed by the Secretariat-General of the European Commission was held on 29th June 2018. Minutes of the meeting are enclosed – Ares(2018)3572339.

### CONSULTATION OF THE RSB

The Regulatory Scrutiny Board discussed the Impact Assessment report on 24th July 2018. The board issued a positive opinion with reservations – Ares(2018)3953436. The comments made the Board were addressed in the revised report; a succinct presentation of how these were reflected in the report is presented in the table below.



www.parlament.gv.at

| RSB Comments | How the updated report addresses the concern | Main sections modified |
|---|---|---|
| **Main considerations** | | |
| **(1) The report does not adequately reflect that the initiative now focuses on illegal content linked to terrorism only. The report does not clearly establish an urgent need to act now at the EU level.** | The report was amended consistently throughout all sections, to clearly focus on the issues raised by terrorist content online.<br><br>The introduction clarifies the state-of-play with regards to other types of content. The evolution of the baseline for other types of illegal content was further explained, while highlighting the focus on terrorist content due the urgency to intervene in this area, as reflected on the calls by the European Council, the Parliament and different international fora. The fact that Europe continues to face high terrorist threat, the role the internet played in the past attacks, as well as uneven progress under voluntary frameworks has been reflected within the repot to establish the urgency of acting on terrorist content only.<br><br>Progress under existing efforts was made more explicit, and stakeholder views were included. | All sections<br><br>Section 2.1 'Scope and further context' presents the rationale in more detail |
| **(2) The objectives do not reflect the balance between the development of the Digital Single Market, reducing terrorist content, and guaranteeing freedom of speech. The report does not adequately explain how the legal basis for acting matches these objectives.** | The presentation of the objectives was further clarified in the report, including:<br><br>- Clarification of the general objective focusing both on supporting trust, innovation and growth in the Digital Single Market and on ensuring a high level of security.<br>- Presentational changes and clarification, at the level of the specific objectives, the balance between (1) facilitating the provision of cross-border services by limiting legal fragmentation, (2) increasing the effectiveness of measures to detect, identify and remove illegal terrorist content online, (3) increased transparency of such measures, (4) improving the ability of competent authorities to intervene, and (5) ensuring the protection of fundamental rights by providing safeguards against over-removal of legal content. | Section 4 'Objectives' |
| | The report also clarifies the choice of legal basis, based on the analysis previously presented in the Annex. It clarifies that Article 114 TEFU is the most appropriate legal basis, explains the rationale and gives further details on how the objectives of the intervention are aligned with article 114 rather than article 83 TEFU.<br><br>It furthermore clarifies how adapting existing instruments, such as the Terrorism Directive, would not achieve the desired objectives of the initiative. | Section 3.1 'Legal basis' |
| **(3) The policy options do not reflect a more** | The policy options were revised to more narrowly focus on a terrorism-related intervention. | All sections of the |

www.parlament.gv.at

| | | |
|---|---|---|
| **tightly scope linked to illegal terrorist content. They are not clear on which service providers they would cover and how they would include smaller platforms in a proportionate way. They do not adequately inform the policy choice.** | The scope of the report was clarified and streamlined:<br><br>- Section 2.1 presents the state-of-play on other types of illegal content and explains the urgency to act in respect to the dissemination of terrorist content. This does not pre-empt further analysis and intervention in other areas.<br>- The problem analysis focuses on terrorist content online.<br>- Objectives, including General and Specific Objectives, are more clearly centred around terrorist content.<br>- The presentation and assessment of the options discarded are aligned with the revision of the Objectives. In addition, the non-regulatory option as well as the horizontal notice-and-action option are presented and discarded.<br><br>The presentation of the options further clarifies that all hosting service providers (HSPs) offering their services in Europe are covered by the provisions. In addition, the provisions requiring proactive measures (to different degrees across the three options) would only cover hosting services exposed to terrorist content and would be proportionate to the level of exposure to terrorist material as well as the economic capacities of the service provider. More granular estimates of the scale and diversity of these services are presented in the problem analysis, and the assessment of the economic impacts builds on these estimates. Annex 4 consistently clarifies that requirements for proactive measures only apply to a more limited number of hosting services, whereas the other provisions cover the population of hosting services. | report, in particular Section 5 What are the available policy options' |
| **(4) The report does not adequately establish that policy options are proportionate with regard to the fundamental right of freedom of expression and what safeguards are provided.** | The report further clarifies the risks each option presents in particular to freedom of expression and information, respect of private and family life and protection of personal data, as well as to the freedom to conduct a business. It clarifies that, the broader the scope of measures to tackle terrorist content online, the higher the risks to interfere on the respective fundamental rights. At the same time, a positive impact on the right to life and right to dignity is presented in particular in relation to measures which enable law enforcement authorities to prosecute terrorist crimes.<br><br>The report explicitly presents the safeguards included in the respective options that mitigate the potential negative effects of fundamental rights and in particular freedom of expression and therefore counter-balances those risks. | Section 6.4 Impacts on fundamental rights |
| **Further considerations and adjustment requirements** | | |
| (1) In line with the services' explanations to the RSB on recent changes in this initiative's scope | As per main consideration (3) above, the scope of the report was more narrowly focused on the issues related to terrorist content online, as reflected throughout the problem analysis, the description of the policy objectives, the presentation, the impact assessment and the | |

www.parlament.gv.at

| | | |
|---|---|---|
| and context, the report should **focus more narrowly on terrorist online content.** It should adjust the problem analysis, the policy objectives and the retained policy options accordingly. To justify the choice of scope, the report should explain why, despite numerous ongoing initiatives, there is a more urgent need to act now on terrorist content. It should report on the experience with measures already taken (voluntary) and on their limitations (e.g. limited participation of Internet platforms in voluntary programmes, hesitant cooperation of online platforms for combatting illegal content, difficult comparability of platforms' reporting). For a better understanding of the context, the report should also show how efforts to combat other illegal content are progressing, and why additional action is less urgent. | comparison of options.<br>The choice of scope is explained up-front in the problem statement, presenting the state of play in the different other areas of policy concern, as well as the urgency to act with regards to terrorist content. | Section 2.1 Scope and further context |
| (2) The report should reshape the general and specific **objectives** to highlight the importance of the functioning of the Digital Single Market, the fight against terrorist online content, and the respect of freedom of speech. It should take into account the narrowing of the scope of the initiative from all illegal content to terrorist content | The general and specific objectives were reshaped to address these concerns:<br>- The General Objective more clearly presents the intent to achieve high level of trust and security to guarantee the smooth functioning of the Single Market.<br>- The Specific Objectives were readjusted to pursue (1) enabling the provision of cross-border hosting service provision by limiting further legal fragmentation, (2) increasing the effectiveness of measures to detect and remove illegal terrorist content online, (3) increasing the transparency and accountability of measures, (4) increasing the ability of authorities to take action against illegal terrorist content and to combat crime, and (5) safeguarding against erroneous removal of content and ensuring that fundamental rights are protected. | Section 4 Objectives |
| (3) On the basis of the redefined objectives, the report should provide a clearer justification for its **choice of the legal base**, i.e. Article 114 TFEU. The report should clearly demonstrate that the objectives can only be satisfactorily achieved under the selected legal base. It could better inform about consequences of selecting this legal base. | The report has been updated to define more clearly, based on the analysis already presented in Annex, the choice of the legal basis i.e. Article 114 TEFU, both by explaining the intervention logic, and in particular, the harmonisation of administrative rules, and case law conducive to the choice of legal basis. It is also expanded on reasons why and intervention based on Article 83 TEFU would not be appropriate to address the desired policy objectives.<br>Furthermore, the report argues more clearly why existing instruments would not achieve the desired objectives, in particular the Terrorism Directive given the focus on criminalisation of terrorist offences as opposed to preventative measures analysed in the Impact Assessment. This would have had a limited impact on the objectives of preventing the dissemination of | Section 3.1 Legal basis |

www.parlament.gv.at

| | | |
|---|---|---|
| | terrorist content in the Digital Single Market at the scale needed to address the objectives. | |
| (4) In the light of the revised focus of the initiative on terrorist online content, the report should also revise the **baseline and the policy options**. The baseline should better project ongoing initiatives and possibly integrate elements now contained in the least ambitious option. The report should detail the policy options, indicating their component measures and highlighting how the options differ from each other. The report could define sub-options such that features of one policy option can also be useful in other policy options (e.g. designation of a competent authority). It should also indicate which type of Internet platforms are covered by each option, and to what extent specific provisions would apply to small service providers. Regarding the least ambitious option, several elements are arguably flanking measures that could be part of the revised options. | The baseline and the policy options were reviewed. The baseline more clearly includes further development of ongoing voluntary measures, whereas additional flanking measures are presented in association with either one of the legislative options.<br>The legislative measures were reduced to the terrorism-specific measures, whereas other horizontal measures are presented earlier in the report and discarded, as they would not, in comparison to the baseline, convincingly address the objectives related to enhancing the detection and removal of terrorist content online.<br>The legislative options are described in several steps and are presented from least to most interventionist. First, the components of the measures are presented in relation to the specific objectives they address; the options are then each described in detail, and the specific differences in the design or intensity of the measures are highlighted across options. For completeness, where the same measure (e.g. designation of a competent authority) is considered in all three options, this is explicitly presented.<br>Not all measures cover all types of HSPs. In particular, the report explains that requirements to take proactive measures for the detection and removal of terrorist content are only required from those hosting services which are exposed to terrorist content. The report also gives further clarity as to the scope of the services covered by proactive measures based on the current estimates (detailed analysis in the problem description, especially p.7).<br>While costs and effects on SMEs are assessed, the options do not include a specific exemption for SMEs, since evidence shows that small companies are equally abused for the dissemination of terrorist content, and such an exemption would impact the ability to pursue the specific objectives of the intervention. However, in particular when proactive measures are concerned, the report clarifies that due account needs to be taken as to the capacity of the HSP to develop and support such measures. | Section 5 Policy options<br><br>Annex 3 Who is affected and how? |
| (5) The report should reinforce the assessment of the impact of the policy options on the development of the Digital Single Market and the fundamental right of **freedom of expression**. The initiative seeks to maintain a delicate balance between the freedom of expression, the respect of the eCommerce Directive and the combat against terrorism. Stakeholders have indicated that the fear of removal of legal content is a major concern to them. For each policy option, the impact analysis should clarify the safeguard measures that aim to ensure the freedom of expression. It | The analysis of the impact on fundamental rights was revised to more consistently present the risks related to proactive measures, in particular in what concerns the risks of over-removal of content through the use of automated tools. Safeguards included under each option were also more clearly presented to highlight the mitigation measures proposed to counter-balance risks related to the fundamental right of freedom of expression and information.<br><br>The report was revised to more clearly centre the specific objectives on the effects on the development of the Digital Single Market, the preservation of the fundamental right of freedom of expression and information, as well as on public security and safety. Consequently, the comparison of options reflects how effectively each option would achieve the respective specific objectives.<br>In addition, the interplay with the e-Commerce Directive was also clarified under the coherence criterion.<br>The report gives further information as to the components of the preferred option on the basis | Section 4 Objectives<br><br>Section 6 Impacts<br><br>Section 7 How do the options compare<br><br>Section 8 preferred option |

www.parlament.gv.at

| | | |
|---|---|---|
| particular, the report should be more specific on the functioning and the precision of the automated content removal systems and the role of human intervention in these systems. The report should also endeavour to better inform the final policy choice by conducting a more rigorous comparison of the options. | of the three options analysed. | |
| (6) The report should better reflect the **views of stakeholders** with regard to the different problems and policy options. It should be transparent about which parts of the consultation are relevant for the narrower focus on terrorist online content | Stakeholder views have been inserted in the relevant sections of the report to better reflect their position on the problems, drivers and options. These now highlight more clearly the justification of focusing on a terrorism-only initiative, as well as on the need to act more urgently in this area, including on the projected evolution of the baseline scenario.<br>Concerns raised by stakeholders on the need to prosecute criminal behaviour and how to address terrorist content online form an integral piece of the EU's general counter terrorism policies, and have been reflected within the report (Introduction and Annex 9). | Section 5 What are the available policy options? |
| (7) The attached quantification tables of the various costs and benefits associated to the options of this initiative need to be adjusted to reflect the changes recommended above. | The tables were adjusted accordingly, in particular to reflect the proposed structure of the options and to more precisely quantify costs for the supporting measures clarified in the report. | Annex 3 and Annex 4 |

www.parlament.gv.at

## EVIDENCE, SOURCES AND QUALITY

### Studies commissioned or supported by the European Commission

ICF, Grimaldi, *The Liability Regime and Notice-and-Action Procedures*, SMART 2016/0039 – forthcoming

VAN HOBOKEN J. et al., *Hosting Intermediary Services and Illegal Content Online* - forthcoming

VoxPol Network of Excellence, http://www.voxpol.eu/

### Data bases

Dealroom database, https://dealroom.co/
SimilarWeb database https://www.similarweb.com/
Orbis database https://orbis.bvdinfo.com

### Selected academic literature


DEMOS, *Islamophobia after the Brussels attack* https://www.demos.co.uk/wp-content/uploads/2016/07/dispatches-Brussels-final.pdf.

GILLES, P. at al, *Terrorist Use of the Internet by the Numbers*, https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9133.12249

KELLER, D. *The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation*, 2017 http://cyberlaw.stanford.edu/blog/2017/04/%E2%80%9Cright-be-forgotten%E2%80%9D-and-national-laws-under-gdpr

LAW, BORDERS, AND SPEECH CONFERENCE: PROCEEDINGS AND MATERIALS, https://cyberlaw.stanford.edu/page/law-borders-and-speech

LEVMORE, S., NUSSBAUM N.C. (eds.), *The Offensive Internet. Speech, Privacy and Reputation*, Harvard University Press, 2010

MANDOLA Project, *Best practice Guide for responding to Online Hate Speech for internet industry*, http://mandola-project.eu/m/filer_public/29/10/29107377-7a03-432e-ae77-e6cbfa9b6835/mandola-d42_bpg_online_hate_speech_final_v1.pdf

SCHMIDT, A., WIEGAND, M., 'A survey of hate speech detection using natural language processing' in Proceedings of the Fifth International Workshop on natural Language Processing for Social Media, Spain, April 2017, http://www.aclweb.org/anthology/W/W17/W17-1101.pdf

VOX-POL, *Violent Extremism and Terrorism Online in 2016: the year in review* at https://www.voxpol.eu/download/report/Year-in-Review-2016_-FINAL.pdf,

WINTER, Ch., INGRAM, H J., 'Terror, Online and Off : Recent trends in Islamic State Propaganda Operations, at https://warontherocks.com/2018/03/terror-online-and-off-recent-trends-in-islamic-state-propaganda-operations/ March 2018


### Public reports and strategy documents


TE-SAT 2018, https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018

United Kingdom's strategy for combatting terrorism, June 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

https://www.gov.uk/government/news/new-technology-revealed-to-help-fight-terrorist-content-online


### Selected media articles


https://www.thetimes.co.uk/article/google-faces-questions-over-videos-on-youtube-3km257v8d

https://www.counterextremism.com/press/counter-extremism-project-unveils-technology-combat-online-extremism
http://www.wired.co.uk/article/chemical-weapons-in-syria-youtube-algorithm-delete-video
https://www.wired.co.uk/article/isis-propaganda-home-office-algorithm-asi
https://www.telegraph.co.uk/news/2018/07/05/facebook-censors-americas-declaration-independence-hate-speech/
https://www.theguardian.com/technology/2017/jan/18/facebook-moderation-racial-bias-black-lives-matter
https://www.telegraph.co.uk/news/2018/07/05/facebook-censors-americas-declaration-independence-hate-speech/

**Company reports, civil society and other sources**

https://blog.twitter.com/official/en_us/topics/company/2018/twitter-transparency-report-12.html
https://newsroom.fb.com/news/2018/04/keeping-terrorists-off-facebook/
https://transparencyreport.google.com/youtube-policy/overview?hl=en
Counter Extremism Project - https://www.counterextremism.com/extremists/anwar-al-awlaki and https://www.counterextremism.com/press/counter-extremism-project-unveils-technology-combat-online-extremism
https://www.microsoft.com/en-us/photodna
The Santa Clara Principles on Transparency and Accountability in Content Moderation, 7 May, 2018.

**Selected case law**

French Supreme Court, 12 July 2012, no. 11-13.666, 11-15.165/11-15.188, 11-13.669
C-18/18, Glawischnig-Piesczek (Case pending)
C-380/03 Germany v European Parliament and Council, judgment of 12 December 2006.
Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-4989,
C-101/01 Lindqvist [2003] ECR I-12971
C-70/10 (SABAM v Scarlet)
C 360/10 (SABAM v Netlog NV)
ECHR, Application no. 24683/14 ROJ TV A/S against Denmark
Hizb ut-Tahrir and Others v. Germany, No. 31098/08
Kasymakhunov and Saybatalov v Russia, No. 26261/05 and 26377/06
Gerechtshof Amsterdam, 24 June 2004, 1689/03 KG, Lycos gegen Pessers.
Zeran v AOL, 129 F.3d 327 (4th Cir. 1997).
Antwerp Civil Court, 3 December 2009, A&M, 2010, n.2010/5-6
President of the Brussels Court (NL), n 2011/6845/A, 2 April 2015
OLG Karlsruhe Urt. v. 14.12.2016 – 6 U 2/15
GRURRS 2016, 115437
Milan Court of Appeal, R.T.I. v. Yahoo! Italia, n. 29/2015;
Rome Court of Appeal, RTI v TMFT Enterprises LLC, judgment 8437/2016 of 27 April 2016
Turin Court of First instance, judgment 7 April 2017 No 1928, RG 38113/2013, Delta TV v Google and YouTube
Supreme Court of Hungary Pfv.20248/2015/9.
Supreme Court, OGH 6 Ob 178/04a.
Judgement of Appellate Court in Wroclaw of 15 January 2010, I Aca 1202/09.
Judgement of 15 April 2014, ECLI:NL:HR:2014:908 (interpretation Art. 54a Sr).
LG Leipzig, judgement of 19 May 2017 (05 O 661/15).

# Annex 2: Stakeholder consultations and feedback

## 1. THE STAKEHOLDERS ENGAGEMENT STRATEGY

The Commission has consulted broadly on issues related to fighting illegal content online, specifically on illegal content hosted by hosting service providers (HSPs). First, preceding the Communication on online platforms, a wide consultation led to a clearer definition of the **problem space** and the start of an in-depth fact-finding exercise. Second, a series of meetings and a consultation on the inception impact assessment published on the 1st March 2018 informed the **problem definition** and led to **preliminary policy options**. Finally, an open public consultation, a Eurobarometer survey and meetings with Member States to review their replies to questionnaires on the Recommendation and way forward contributed to the **design and testing of policy options**. The understanding of the evolution of the problem is also based on past open public consultations, notably in 2010 and 2012.

The Commission also organised targeted consultations over the past year and, including on terrorist-specific issues and horizontal considerations. In addition, the Commission's services have met or interviewed through bilateral meetings a series of stakeholders, as listed here below.

In developing the stakeholder engagement strategy, the stakeholder mapping included: (i) a spectrum of online platforms fitting into the category of HSPs (different company sizes, established in Europe or international), (ii) trusted flaggers (with expertise in public policy areas or with commercial interests, namely in the intellectual property arena) (iii) citizens (through consumer organizations and digital rights civil society representatives), and (iv) academia.

The different consultation tools as well as brief summaries of their results are described here-below:

- Preliminary results of the Eurobarometer on illegal content online (June 2018)
- Summary of the open public consultations (June 2018)
- Summary of other, targeted consultations (horizontal issues)
- Summary of other, targeted consultations (terrorist content-specific)

## 2. FLASH EUROBAROMETER 469 ON ILLEGAL CONTENT ONLINE (JUNE 2018)

The Eurobarometer questionnaire was conducted in June 2018 through phone interviews run to a random sample of 33,500 EU residents.

Preliminary data68:

Is the Internet safe for its users?

- 65% of respondents considered that the Internet is not safe for its users. 31% disagree.
- 90% of the respondents consider that arrangements should be in place to limit the spread of illegal content online. 8% disagree.
- 85% of the respondents said freedom of expression should be protected online. 12% disagree.

68 Full report expected to be published in September 2018



www.parlament.gv.at

- 61% of respondents claim to have seen accidentally some illegal content online - 6% of respondents have seen child abuse material, 6% terrorist content, 26% pirated content, 27% counterfeit goods, 29% hate speech, 41% scams and fraud, 10 % other.

Notice and takedown

- On the effectiveness of hosting services in tackling illegal content, no clear trend: 44% agree while 39% disagree.
- 40% of the respondent having seen illegal content took an action - 8% alerted the police, 9% contacted directly the uploader, 21% contacted the HSP.
- 45% of reported content was taken down, 20% was kept online, 8% was slightly modified, 7% kept online with more restricted access.
- 64% of respondents were satisfied with the way the HSP handled the notification.
- 75% considered that the user should be able to appeal the decision when the Internet hosting service removes content uploaded by a user.

Over-removal

- 5% of respondents tried to upload or post content online which was legal but which was wrongly blocked or removed by the internet hosting service. Justification: 1% for terrorism content, 2% child sexual abuse material, 5% hate speech, 17% pirated content, 4% counterfeit, incompatibility with the Terms and Conditions.

Need for action & options

- 86% considered that Internet hosting services should process all notifications they receive and assess the legality of the content. 9% disagree.
- 90% of the respondents considered that hosting services should immediately remove content flagged as illegal by competent authorities and law enforcement bodies, 7% disagree.
- 85% of respondents considered that Internet hosting services should immediately remove content flagged as illegal by organisations with proven expertise on the topic. 10 % disagree.

## 3. OPEN PUBLIC CONSULTATIONS

The Commission has conducted several open public consultations on the related issues, first in 2010 in the context of the evaluation of the e-Commerce Directive, in 2012, with a focus on notice-and-action procedures for all types of illegal content, then in 2016, part of the broader open public consultation on online platforms and, finally, in 2018.

### Open Public Consultation on measures to further improve the effectiveness of the fight against illegal content online (30 April – 25 June 2018)

The open public consultation was launched on the 30th April and ran for 8 weeks. The shorter consultation period compared to the 12 weeks period usually applied by the Commission was defined in order to ensure that its outcome could be used for the preparation of this Impact Assessment. To mitigate the impact that a reduced timeframe could have on the participation in the consultation, the Commission disseminated the call for contributions widely, including through the targeted discussions and consultations. In addition, the Commission ran campaigns on mainstream social media, including by targeting specific audiences (general public; professionals representing HSPs, civil society).



www.parlament.gv.at

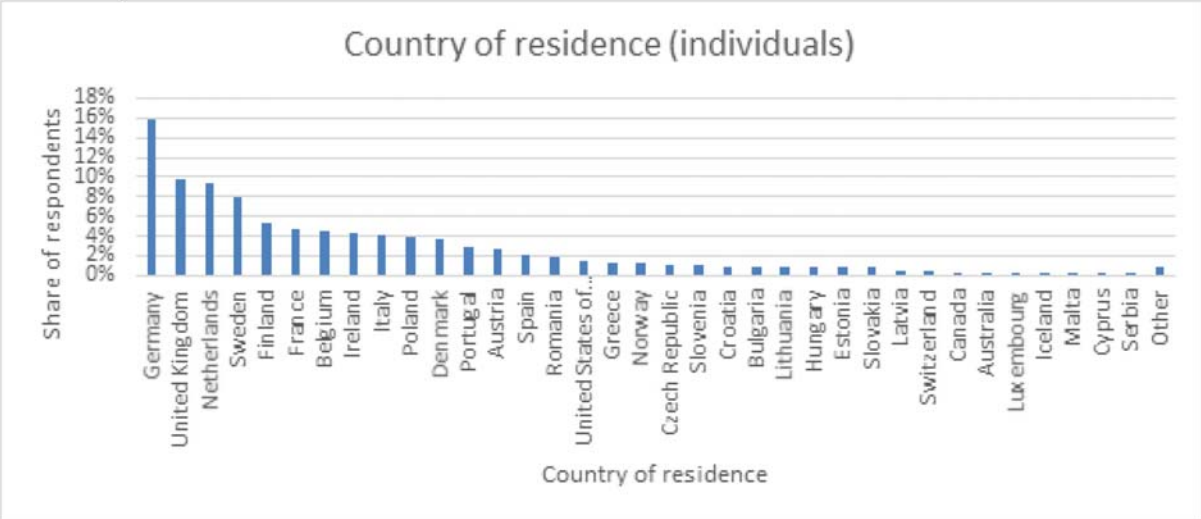
*3.1.1 Demographics*

The public consultation has received a total of 8,961 replies, of which 8,749 are from individuals, 172 from organisations, 10 from public administrations, and 30 from other categories of respondents.

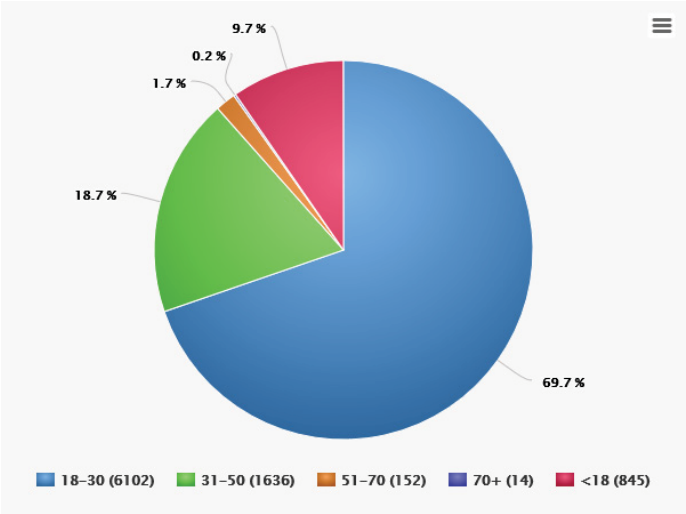
Individuals

Respondents were profiled as internet users – in particular, users of specific types of hosting services. They were generally heavy users of such services, significantly more so than respondents sampled in the Eurobarometer. Most intensely used services were audio/audiovisual media sharing platforms, e-commerce market places, file sharing and transfer services, social media platforms, or blog-hosting platforms.

Where they are from?




Age segmentation



Organisations

a) 18 HSPs and 4 major business associations replying on behalf of online HSPs, including one association representing specifically start-ups.

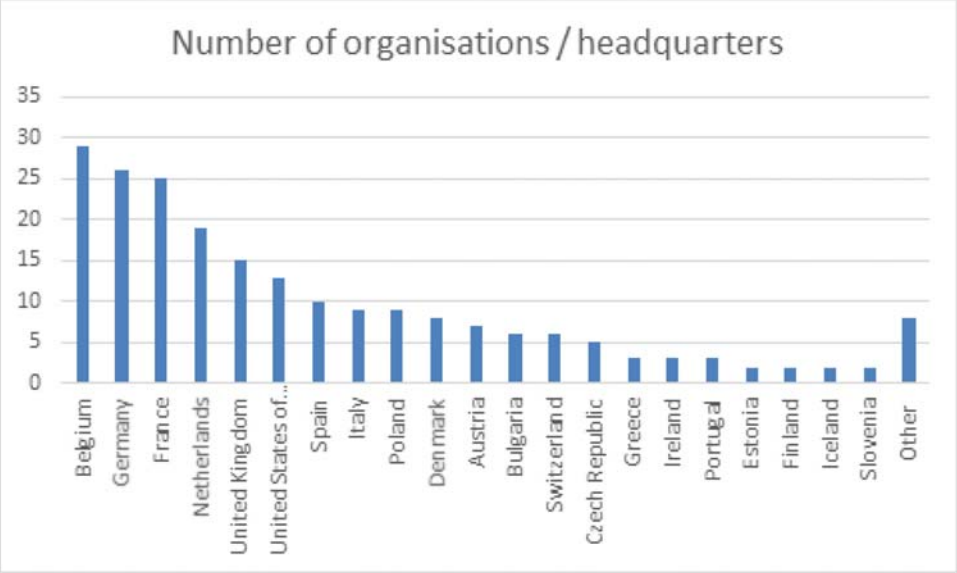
b) 10 competent authorities, including law enforcement authorities, Internet referral units, ministries or consumer protection authorities (2 from law enforcement authorities investigating criminal activities, 3 from national governments, 1 from consumer protection authorities and 4 from other specialised national bodies).

c) 39 replies have been submitted by not-for-profit organisations identifying and reporting allegedly illegal content online, including 3 from non-EU countries. 21 of the respondents reported to be flagged as "trusted flaggers" with a privileged status given by HSPs.

d) 10 organisations or business representing victims (mostly concerning IPR infringements)

e) 76 replies from IT companies associations, other industry associations and other stakeholders such as the Council of Europe, one political party, civil rights advocates and IP right holders, whose views are reflected in a discrete paragraph above.

f) 11 research or academic organisations:




*3.1.2 Overview of responses*

3.1.2.1 Hosting services

Overall, hosting services did not consider that additional regulatory intervention would be conducive to better tackling illegal content online, but supported, to a certain degree, voluntary measures and cooperation.



www.parlament.gv.at

Associations representing large numbers of HSPs considered that, if legal instruments were to be envisaged at EU level, they should in any case be problem-specific and targeted. They broadly supported further harmonisation of notification information, but expressed substantial concerns as to the feasibility of establishing strict time limits on takedown of content (from upload), pointing to over burdensome processes especially for SMEs, and to general incentives of over-removal. They also pointed to the need to have a cautious approach concerning proactive measures, highlighting the general cooperation and good results in the actions taken through the sector specific voluntary dialogues.

Contributions from different companies highlighted the differences in available capabilities across businesses, as well as the different incentives and technical possibilities depending on their value propositions. Companies were also generally open to cooperation including with government agencies or law enforcement flagging illegal content.

While big companies reported using, besides notice and action systems, proactive measures, including content moderation by staff, automated filters and, in some cases other automatic tools to flag to human reviewers content potentially illegal, responses also showed that smaller companies are more limited in terms of capability. Amongst the respondents, it seemed that SMEs were generally relying on notices for flagging all types of illegal content. One SME described difficulties in implementing semi-automated tools – without having access to the tools developed by the big industry players – and the trade-off experienced between increasing performance in removing illegal content, and the higher incidents of erroneous removal of legitimate content of their users.

#### 3.1.2.2 Competent authorities, including law enforcement authorities, Internet referral units, ministries or consumer protection authorities:

The main concerns expressed by those public authorities who responded were about illegal commercial practices (3 respondents), child sexual abuse (2 respondents) and copyright (2 respondents).

6 respondents declared to identify and refer illegal contents to hosting service providers, among which 4 on the basis of national law. Illegal content was mainly detected through trusted flaggers or by means of direct reporting by the right holders. For instance, one public authority declared that under national law, in case of infringement of copyright, the only party entitled to report the violation of such right is the right holder whose right has been infringed. Automated tools are generally not used by the public authorities responding to the consultation.

Public authorities outlined the increasing difficulty to judge which content is harmful or illegal and which is not. Other public authorities reported their difficulty to identify the sources of the illegal content online and therefore the lack of evidence for any related judicial action. The turnaround time for removing illegal contents is considered as a critical point as well.

Some respondents required a clear and precise legislation which would take into account the different actors that operate in the EU, whereas others emphasised the importance of having strong and effective cross-border cooperation between the national regulatory authorities.

#### 3.1.2.3 Trusted flaggers, notifiers with a privileged status and organisations representing victims

Amongst the respondents, 26 were mainly concerned with copyright infringements, 5 with child sexual abuse material and 3 with illegal commercial practices online.

Concerning the tools used to detect copyright infringements, 22 reported to use content monitoring and report by their own staff, whereas 18 declared to use automated tools. In such respect, more than half of the respondents reported that both public and private investments in research and development would be necessary to uptake and deploy automated tools for the removal of illegal contents online.

Some respondents warned as to the challenges in using automated tools and claimed that any technological system put in place to intercept content must be able to recognize new material quickly and accurately to account for changes. To ensure such result, human assessment had to be included in the decision-making process.

Furthermore, the not-for-profit organisations considered the standardised access and user friendly interfaces for reporting illegal content to be very effective and enabling HSPs to make diligent decisions. Conversely, the explanation of reasons and grounds of illegal content and anonymous notices were reported as being inefficient for some types of illegal content such as IPR infringements.

Amid the respondents, 21 declared the setting of time limits for processing referrals and notifications from trusted flaggers as being important to support cooperation HSPs and trusted flaggers.

#### 3.1.2.4 Civil society organisations representing civil rights interests:

Despite having issues with the current framework, especially in terms of transparency of the processes for removing illegal content or contesting a removal, civil society organisations representing civil rights interests expressed concerns about the impact proactive measures or new legislative measures may have on freedom of expression and information. In this context, they were concerned that decisions by platforms about controversial content according to their terms of service in a non-transparent way may impact the rule of law and ultimately endanger freedom of expression.

Respondents agreed with reinforcing public authorities' capabilities in fighting illegal content on-line and were not particularly in favour of attaching privileges to trusted flaggers or imposing on platforms an obligation to report to law enforcement bodies all alleged illegal content. Like respondents in other groups, they were not keen on out-of-court dispute resolution procedures either.

Several civil society organisations (and some respondents from other groups as well) considered that the focus should be put on searching and prosecuting providers of illegal content rather than on removing illegal content as this might have a negative impact on users' rights, whilst they also acknowledged that reaching and prosecuting the perpetrators is not always possible.

#### 3.1.2.5 IP rights holders

Intellectual rights owners and their associations surfaced via different respondent groups in the public consultation. They include publishers, film and music labels, media and sports companies, as well as trademark owners.

In their view, the voluntary approach is rather ineffective and it puts companies doing more than required by law at a competitive disadvantage. Brand owners noted that counterfeiting does not only damage industry rights but consumer safety as fake products are often produced without complying with security standards. They criticized the enforcement of transparency obligations in Directive 2000/31/CE and considered that the "follow the money" approach has been difficult to implement. They claimed for a system of shared enhanced responsibilities for intermediaries supported by a stronger legal framework. Establishing "stay-down" obligations features in individual submissions too. Companies holding rights in sports events contended that platforms should enable them to take down content in real time.

#### 3.1.2.6 Other industry associations

This group includes 76 replies from IT companies associations, other industry associations and other stakeholders such as the Council of Europe, one political party, civil rights advocates and Intellectual Property (IP) right holders.

As other groups of, respondents reported low levels of feedback from platforms on notices to take down content. When content was removed, it was mainly done within days. One respondent noted that it is easier to report user generated content such as hate speech comments than false advertisements.

Although the majority of respondents saw a need for some level of EU action, many industry associations advised against complex regulations. In this regard, some of them highlighted that policies oriented along capabilities of large corporations create barriers to market entry and innovation. Prominent IT companies' associations underlined that the variety of policies and voluntary schemes in place should be given time to prove their results and be properly assessed before legislating. In their view, self-regulation and public-private cooperation should in any event be stepping-stones towards ensuring illegal content online is kept at bay. One respondent was however favourable to tackling terrorist content by legislating.

With the caveat of costs for small business, that some remind in their contributions, they are supportive of proactive detection tools counterbalanced by safeguards like transparency and the "human-in-the-loop" principle. They also agreed with the need for arrangements to prevent illegal content from spreading, but preferred best practice, voluntary sharing of databases or software tools to ensure the deployment of automated tools across HSPs. They were also in favour of standardising notice and action procedures, with a relevant industry association opposing this view.

#### 3.1.2.7 Research or academic organisations:

Like other groups, respondents considered that different kinds of illegal content needed different frameworks. As regards the notice and action procedure, one respondent noted that outside Europe the take-down mechanism is unclear and sometimes non-existent.
They pointed to the lack of real incentives (if not sporadic media attention) companies might have to deal with counter-notices, whereas non-treatment of notices can more easily lead to legal consequences. They also underlined that existing counter-notice procedures are by and large

underused, with the few companies who do report on counter-notices listing on a yearly basis only one-to-two digits numbers.[69]

They were particularly concerned about the use of automated tools in detecting illegal content online and advised caution when incentivising hosting services to apply proactive measures, and underlined the need for human rights safeguards and transparency to the process of detecting and removing alleged illegal content online.

They side with some other respondents in giving priority to public authorities' notices over trusted flaggers' ones; preferring public investments in research and development and in favouring publicly supported databases for filtering content, training data or technical tools.

#### 3.1.2.8 Individuals

**Is the internet safe?**

- Over 75% of individuals70 responding considered that the Internet is safe for its users, and 70% reported never to have been a victim of any illegal activity online. Where they were victims, this concerned, for nearly 12%, some form of allegedly illegal commercial practice.

**Measures to take down illegal content**

- Regarding notice and action procedures: 33% of the individual respondents reported to have seen allegedly illegal content and have reported it to the hosting service; over 83% of them found the procedure easy to follow.
- The overwhelming majority of respondents to the open public consultation said it was important to protect free speech online (90% strongly agreed), and nearly 18% thought it important to take further measures against the spread of illegal content online. 70% of the respondents were generally opposed to additional measures.

**Over-removal**

- 30% of the respondents whose content was wrongly removed (self-reported) had issued a counter-notice.
- 64% of the respondents whose content was removed found both the content removal process, and the process to dispute removal as lacking in transparency.

**Transparency and information**

- Nearly half of the individuals who had flagged a piece of content did not receive any information from the service regarding the notice, while one third reported to have been informed about the follow-up given to the notice. For one fifth, the content was taken down within hours.
- One fifth71 of the respondents who had their content removed from hosting services reported not to have been informed about the grounds for removal at all.

69 ICF study (forthcoming). Comparative analysis of transparency reports of several companies points to negligible numbers of counter-notices per year.
70 Out of 8749 responses from individuals
71 450 out of nearly 2000

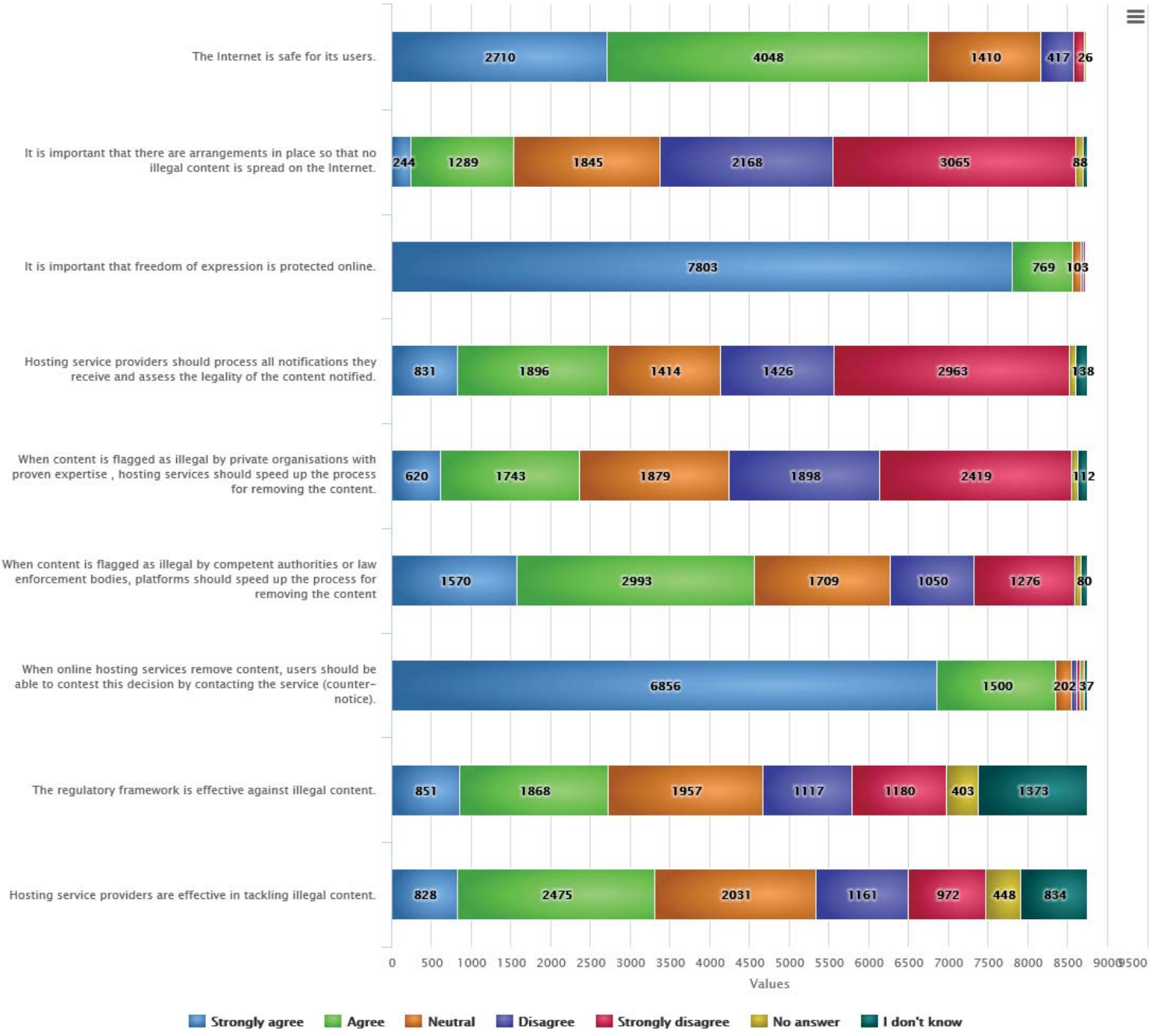


www.parlament.gv.at

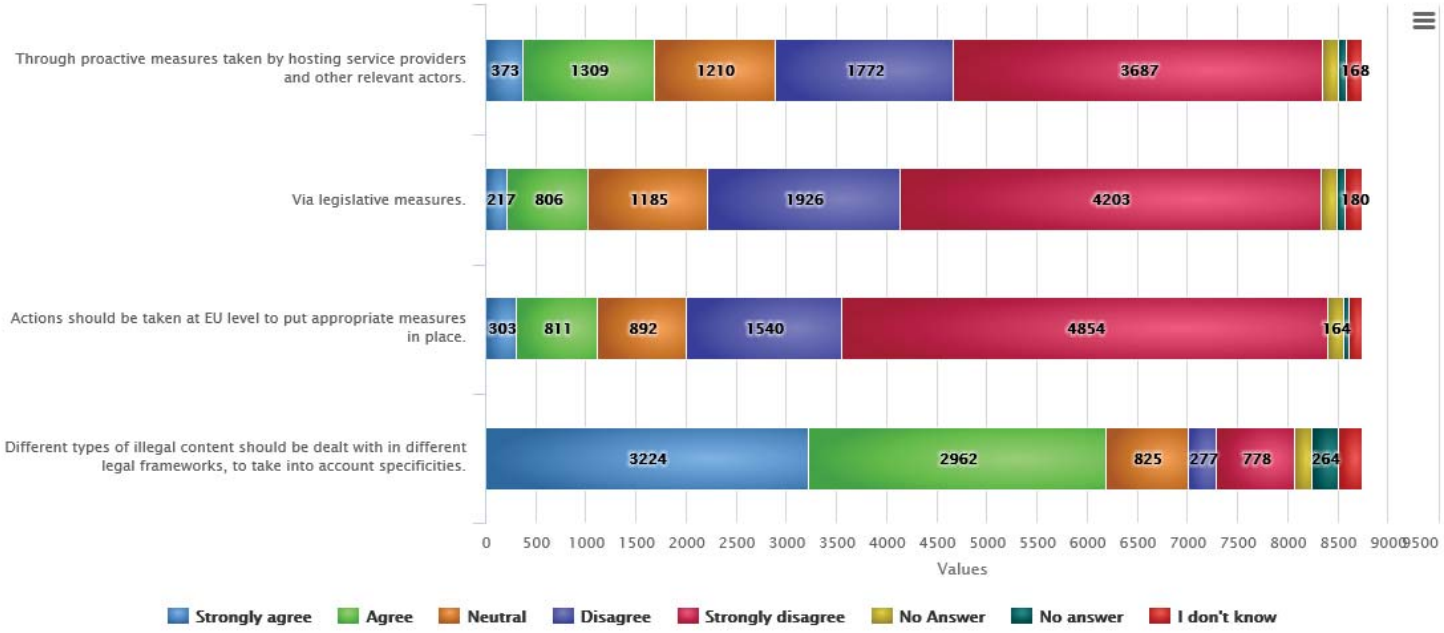
**Need for action & options**

- 30% of respondents considered that the current legal framework for tackling each of the different types of illegal content was effective. Nearly 40% found that actions currently taken by HSPs are effective.
- Nearly half of the respondents considered that hosting services should remove immediately content notified by law enforcement authorities, whereas 25% opposed such fast-processing.
- Half of the respondents opposed fast removal for content flagged by organisations with expertise (trusted flaggers), other than law enforcement, but 25% agreed with such fast procedures.

To what extent do you agree with the following statements?



In your opinion, is there a need for further measures to tackle illegal content online?



### 3.2 Open Public Consultation on "Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy" (September 2015-January 2016)

The consultation received 1,034 replies, although one of them (an advocacy association) included 10, 599 individual contributions.72 Its results as far as the liability of intermediary service providers is concerned, can be summarized as follows:

- The majority of respondents think that the existing liability regime in the e-Commerce Directive is fit-for-purpose.
- The majority of respondents demanded either clarification of existing or the introduction of new safe harbours. The most often discussed safe harbour was hosting (Article 14), in particular its concept of "passive hosting". When asked specifically about this concept, many respondents complained rather about the national interpretations of this concept. Several supported clarification by means of soft-law measures such as recommendations issued by the European Commission.
- 71% of respondents consider that different categories of illegal content require different policy approaches as regards notice-and-action procedures, and in particular different requirements as regards the content of the notice.
- 61% of online intermediaries state that they have put in place diverse voluntary or proactive measures to remove certain categories of illegal content from their system.
- 61% of the respondents are against a stay down obligation.
- 77% of the respondents are in favour of increasing transparency with regard to the duties of care for online intermediaries, with regard to the general content restrictions policies and practices by online intermediaries.
- 82% of the respondents are in favour of a counter-notice procedure.
- Views were particularly divided over (i) the clarity of the concept of a 'mere technical, automatic and passive nature' of information transmission by information society service providers, (ii) the need to clarify the existing categories of intermediary services (namely mere conduit/caching/hosting) and/or the potential need to establish further categories of intermediary services, (iii) the need to impose a specific duty of care regime for certain categories of illegal content.

### 3.3 Open Public Consultation on notice-and-action procedures73 (2012)

- The public consultation revealed broad support for EU action (among all categories of respondents). More specifically it revealed strong support for clarification on certain notions of the e-Commerce Directive, for rules to avoid unjustified actions against legal content (in particular consultation of the content-provider and counter-notification by the content provider), for requirements for notices and for feedback to notifiers.
- However, respondents appeared to be divided on the final instrument of the initiative.
- 48% considered that if an HSP takes proactive measures it should be protected against liability that could result ("Good Samaritan clause").
- 53% affirmed that action against illegal content is often ineffective and lacks transparency.

72 The full report of the results of this public consultation can be downloaded from https://ec.europa.eu/digital-single-market/en/news/full-report-results-public-consultation-regulatory-environment-platforms-online-intermediaries

73 http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet/summary-of-responses_en.pdf (2013)

- 55% considered that concepts of "hosting", "actual knowledge" and "awareness" unclear.
- 64% considered that HSPs often take action against legal content.
- 66% considered that a notice should be provided by electronic means.
- 71% considered that HSPs have to consult the content providers first.
- For 72% of the respondents, different categories of illegal content require different policy approaches.
- 77% considered that the sender of the notice should be identified.
- 80% considered that there should be rules to avoid unjustified or abusive notices.
- 83% considered that the notice should describe the alleged illegal nature of the content.

### 3.4 Open Public Consultation on the e-Commerce Directive[74] (2010)

Full report available at http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf - see in particular questions 52 to 73.

## 4. OTHER, TARGETED CONSULTATIONS AND ENGAGEMENT ACTIVITIES

### 4.1 Bilateral meetings:

In the course of the preparation of this Impact assessment, the Commission has engaged with the following stakeholders through bilateral meetings that took place between 2017 and 2018:

- ACT – Association of Commercial Television in Europe: they gather and represent the interests of private broadcasters in 37 European countries.
- ASI Data Science: they are a company based in the United Kingdom that offers artificial intelligence solutions to make sense of data and generate business value. They have developed a tool for UK Home Office to identify and remove ISIS online propaganda.
- Center for Democracy and Technology: it is an advocacy organisation headquartered in Washington (USA) working to preserve users´ privacy online, freedom of expression and controls over government surveillance of the Internet.
- Cloudflare: it is a U.S. company that provides content delivery network services, distributed denial of service attack (DDoS) mitigation, Internet security and distributed domain name server services, sitting between the visitor and the Cloudflare user's hosting provider.
- CNNum: the « Conseil national du numérique » is an expert body advising the French Government on issues relating to digital issues, in particular issues and prospects for the digital transition of society, the economy, organizations, public action and the territories.
- Cyber Data Alliance
- eBay: it is a U.S. multinational e-commerce corporation that facilitates consumer-to-consumer and business-to-consumer sales through its marketplace.
- EDIMA: it is a European trade association representing online platforms and other innovative tech companies in Europe that engages with policy-makers on issues that affect their business and the innovative sector.
- Facebook: it is an online social media and social networking service founded by Mark Zuckerberg in 2004.

74 http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf - see in particular questions 52 to 73.



www.parlament.gv.at

- GESAC (European Grouping of Societies of Authors and Composers): it manages the rights of their members' works and represent them in negotiations to secure fair remunerations for creators
- Google: it is a U.S. multinational technology company that specializes in Internet-related services and products, which include online advertising technologies, search engine, cloud computing, software, and hardware.
- King's College London: it is a public research university located in London, United Kingdom, and a founding constituent college of the federal University of London.
- Mozilla: it is free software community founded in 1998. Mozilla community is supported institutionally by the not-for-profit Mozilla Foundation and its tax-paying subsidiary, the Mozilla Corporation. Mozilla's products include the Firefox web browser, Thunderbird e-mail client, Firefox OS mobile operating system and others.

- MATCH: it is the global leader in the dating business. Their brands include Tinder, Match, Meetic, Love Scout 24 and others.
- MPAA (Motion Picture Association of America) is a U.S. trade association representing the six major film studios of Hollywood. It advocates for effective copyright protection and expansion of market access.
- Nike: it is a U.S. multinational corporation engaged in the design, development, manufacturing, and worldwide marketing and sales of footwear, apparel, equipment, accessories, and services.
- Sectorial Social Dialogue Committee for Audiovisual: it is a committee of the International Federation of Actors that brings together the European social partners in the Audiovisual sector to discuss issues related to social dialogue, gender equality, skills and training and piracy.
- SNAP: it is a U.S. based company running Snapchat, a multimedia messaging app used globally.
- Warner Bros: a subsidiary of AT&T's Warner Media, it is one of the "Big Six" major American film studios.

### 4.2 Reactions to the Communication on tackling illegal content online COM(2017) 555 final, of 28th September 2017 and to the Recommendation on measures to effectively tackle illegal content online C(2018) 1177 final, of 1st March 2018:

- EDRi's paper "A coherent and rights-based approach to dealing with illegal content", of 20th October 2017: they propose the Commission to adopt at least three workstreams to create a harmonised and coherent approach to illegal content online: to develop an understanding of the fundamental rights framework in this complex policy area; to establish a structure for learning from the experience of the past 20 years, and to establish a clear methodology for developing effective and predictable frameworks for addressing illegal content that respect fundamental rights.75
- Several Members of the European Parliament's letter of 5th December 2017: they urge the Commission to assess the impact of automated detection tools, whose use the Communication encourages, on freedom of expression. At the same time, these MEP call on the Commission

75 https://edri.org/files/letter_coherent_rightsbasedapproach_illegalcontent_20171020.pdf

to develop procedural requirements for notice and action to prevent unjustified restrictions of speech by private HSPs. Finally, they seek the Commission's attention to the international resonance of EU policies and warn against proposing actions that could be used to vindicate questionable laws to supress freedom of speech outside the EU.

- Artisjus' message of 5th February 2018
- Joint letter signed by Allied for Start-ups, CCIA, CDT, Ecommerce Europe, EDiMA, EDRi, Developers Alliance, ETTSA, EMOTA and EuroISPA, of 13th February 2018: they ask the Commission to refrain from issuing an over-arching Recommendation on illegal content online without evidence of new major incidents that justify further action. They also criticize the Commission for doing so without engaging with business and civil society on best ways to tackle it.
- Several trademark owners´ letter of 20 February 2018.
- eBay's comments on Recommendation C(2018) 1177 final: the company reckons that the Recommendation has neither taken into account long-standing legal principles applying to online intermediaries or the implications of complying with the recommendations. It provides detailed objections to them and suggests maintaining a horizontal liability regime while addressing the specific needs of each type of illegal content in a multi-stakeholder fashion.

### 4.3 Feedback of Member States on the application of Recommendation on measures to effectively tackle illegal content online C(2018) 1177 final, of 1st March 2018 (E-Commerce Expert Group meeting held on the 14th June 2018)

On the 14th of June 2018, DG CONNECT convened the 19th E-Commerce Expert Group meeting to gather information on the implementation of the Recommendation on measures to effectively tackle illegal content online at a national level. Experts representing 20 Member States attended the meeting and illustrated the measures and steps each Member State has taken or intended to take to implement the Recommendation. The discussion was based on a questionnaire sent to national authorities before the meeting.

The main outcomes of the meeting are summarized hereunder:

- Administrative and organizational measures: no concrete measures have been adopted yet. National authorities are still identifying further steps to take. Some countries consider the area sensitive and difficult to regulate – in their views, a sectorial approach shall be adopted given that each type of content can have a different level of threat.
- Out-of-court dispute settlement mechanism: no specific out-of-court dispute mechanism adopted in the Member States attending the meeting. The already existing traditional dispute settlement mechanisms are generally considered sufficient.
- Points of contact for matter related to illegal content online and cooperation with HSPs: Member States reported that, in general terms, the cooperation between governments and HSPs' points of contact works well. Big platforms are rather active and willing to collaborate. One expert reported the difficulty encountered with small HSP that were generally not willing to collaborate. Overall, Member States noticed a clear progress in the cooperation with the different stakeholders.
- Fast-track procedures: the national experts attending the meeting reported that there are no fast-track procedures provided by their national laws except for one Member State which has



www.parlament.gv.at

a simplified procedure for cases of child sexual abuse. Most of the experts were of the view that there is no need to implement such a procedure.

- Participants also discussed the risks and benefits of establishing strict timeframes for content removal by hosting service providers.

Case law: Austria reported the still pending *Glawischnig* case concerning, inter alia, the geographical reach of the deletion of illegal content online.

### 4.4 Feedback on the Inception Impact Assessment76 (2nd to 30th March 2018)

A total of 146 replies were submitted. Half of them are identical copies of a submission representing Ukranian journalists.

The replies represent broadly the whole stakeholder spectrum: from businesses representing the Internet industry and their associations to rights holders and other trusted flaggers active in the fields of hate speech and terrorism, the advertising industry, and representatives from the civil society (digital rights associations) and academia.

Some common comments can be identified:

- General sentiment against strict timeframes for removals, with the exception of IP right holders for whom speedy take-down is of essence.
- Broad support for voluntary cooperation frameworks in place, since they have yielded positive results. Hence, a call not to hinder its development, coupled with a call to extend the cooperation to smaller companies.
- Call for caution in pushing hosting services to apply automatic tools to detect and remove content for the risk of over removals and anticompetitive effects on SMEs.
- Need for further transparency on platforms' content policy implementation.
- Many expressed the view that different types of content require a different set of actions.

Other views expressed include:

- Internet business associations, individual intermediary service providers and advertising services preferred the baseline option. These stakeholders considered that Directive 2000/31/EC remained a strong and flexible framework that should be respected. They shared the view that intermediary service providers need to be protected from liability when they take proactive measures.
- Trademark and copyright owners preferred horizontal legislation addressing targeted issues. They decried anonymity on the Internet, and demanded that a “stay down” obligation be created. Besides, they stood for the use of automatic tools to detect illegal material, to prevent its re-uploading and to avoid repeat infringers. Moreover, they claimed trusted flaggers be allowed to take down content live.
- Digital rights associations preferred the baseline option and flagged the risks entailed by measures such as automatic filtering for the preservation of fundamental rights.
- Non-governmental organisations called for a detailed definition of “illegal content online” and for fast-track procedures for notifications provided by public authorities.

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



www.parlament.gv.at

- Member States participating underlined that further measures should not undermine Directive 2000/31/EC. They also highlighted that it is not enough to remove illegal content, and that the approach to online content should not impede on the ability to prosecute the underlying crime/offense.

### 4.5 Meeting with trusted flaggers on the 7th February 2018:

Commissioner Gabriel called this meeting with trusted flaggers to listen to their feedback on the September Communication on illegal content.

The meeting gathered expert organisations working in radically different areas: public policy areas such as terrorism, illegal hate speech, Child Sexual Abuse Material (CSAM), and commercial interests in the area of intellectual property infringements.

The exchange of views highlighted stark differences between them, i.e.: some flag content against companies' terms of service and others only illegal content; illegality of the content is easier for IP right holders and CSAM hotlines to assess than for organisations fighting hate speech; some coordinate notifications at EU level to avoid duplication of efforts (as in the area of terrorism) while CSAM hotlines and hate speech organisations tend to operate nationally.

However, all the trusted flaggers face some common problems. For example: difficulties to interact with smaller platforms; the frequent reappearance of content already taken down, and the need to deal with the roots of the problem, as removing the illegal content is only treating the symptom.

Views expressed can be summarized as follows:

- Cooperation network: trusted flaggers welcomed the informal exchanges and learning opportunities that they bring along but there was no enthusiasm about the creation of a formal cooperation network at EU level.
- Accreditation system: the situation at present is very fragmented, with each platform deciding which organisation is trustworthy for them according to non-published criteria. Views were divergent although most did not see a need for an accreditation system.
- Cooperation with platforms: whereas as trusted flaggers pursuing public interests were satisfied with their relationship with online platforms, trademark and copyright owners were frustrated by the reappearance of content already taken down, disparity of speed of removals and poor feedback received, among other things.
- Areas for improvement in a legislative instrument: for all, bringing a certain degree of standardisation to notifying procedures. For IP and trademark owners, granting priority to notices sent by trusted flaggers; providing more transparency on actions taken by platforms to right holders; ensuring real expeditious removal or, where appropriate, real-time removals; standardise notification procedures; laying down measures against repeat infringers, and above all, enshrine the "stay down" principle.

### 4.6 High level meeting with online platforms held on the 9th January 2018:

The aim of the meeting was to receive confirmation of platform's commitment to the implementation of the Communication and to ask them to show effective progress on the removal of illegal content. The meeting was chaired by 5 Commissioners and attended by more than 20 companies of all sizes.

The meeting was held under the under Chatham House rules. The following views were expressed in online platforms´ interventions:

- The availability of illegal content on digital platforms undermines trust of users, which is very harmful for a business model based on trust.
- Satisfaction with the current liability regime of the e-Commerce Directive, although they are mindful of their responsibility towards society.
- Satisfaction with the progress made in removing illegal content in the areas of child sexual abuse material, illegal terrorist content and illegal hate speech. The key of success has been cooperation between government, industry and civil society.
- Deciding if content is illegal or not is a challenge, in particular in the area of hate speech. This challenge is exacerbated by legal imposition of very short deadlines for reaction.
- The volume of online content intermediated is a challenge too.
- Protecting fundamental rights, in particular freedom of speech and people's privacy, is also a challenge for companies when removing illegal content;
- There was a call for a distinction between two categories of "illegal content" when proposing any action: illegal goods, especially fakes in e-commerce, on the one hand, and all the other types of illegal content, on the other.
- There are no simple technical solutions to remove illegal content online. Machine learning algorithms are currently used and are very effective, but human intervention is always necessary. Automatisation may work well for certain types of illegal content but not for others. It is also a challenge that algorithms are specific to one language and cannot be easily transferred to others.
- Transparent report is key to measure progress, but on trends and aggregated numbers rather than precise figures.
- Need of international collaboration, open source spirit, and transfer of know-how, data and technology from big to smaller companies, to avoid displacement of illegal content to them and ensure everyone can contribute at best to this common goal of improving effectiveness of the fight against illegal content online.
- Offline measures also are needed as well as improved cooperation with authorities coupled with digital literacy programmes.

### 4.7 Semi-structured interviews with judges across the EU

In total five judges were interviewed over June and July 2017, including representatives from the United Kingdom, Germany, Italy, the Court of Justice of the European Union and the European Court of Human Rights. General views collected through these interviews include:

- Different levels of experience in cases involving intermediary services among Member States. That affects understanding and consistency in applying the liability regime.
- The liability regime is still useful but will require more flexibility as technology evolves. Any replacement of this regime would require a careful balancing of interests.
- Different categories of illegal content should be treated differently.
- Need to decide case-by-case whether an intermediary plays an active or a passive role.
- More clarity and standardisation of minimum requirements of notices would be useful.
- Setting one fixed deadline to take action on notices would not be appropriate.
- Lack of clarity of recital 42 of Directive 2000/31/EC. Uncertainty as to whether the use of algorithmic or automatic process to detect illegal content renders service providers active.

- The use of automated processes is pushing in the direction of a general monitoring obligation. The ban on such obligation is still useful, although for several judges it might become less so in the future.
- Relying on intermediaries to police the Internet is risky. If the Commission wishes to encourage this, it should provide clear guidelines on what content is considered illegal.
- Judges considered that in principle judicial oversight was more appropriate in regards to rule of law than private standards.
- There was calls for new legal processes (such as Internet courts) to allow judges to deal with potentially illegal content online quickly.

### 4.8 Workshop on Digital Platforms and Fundamental Rights, held on 12 June 2017

The panel of 4 experts brought together the expertise from academia, digital platforms and civil rights organisations.

Some highlights of the meeting are indicated below:

- States may breach their positive obligations to promote human rights for their failure to prevent violations of individuals' fundamental rights as a result of privatized law enforcement by online intermediaries.
- Removing illegal content online does not automatically solve the underlying problems. Offline action, including investigation of content removed as illegal, is also needed.
- One of the possible areas of intervention of the EU could be increasing the transparency on how platforms make decisions about fundamental rights. Platforms should make clear and understandable for users the criteria and the procedures that they follow, the remedies available for users in case of disagreement, the amount of resources put in place to take those decisions. Information about the results would be also crucial, both at individual user level and social reporting.
- Lack of proper reasoning to notices makes it hard for platform to deal with them. An additional difficulty is their global operation versus divergent regional regulations on what is considered as allowed or not.
- Too much pressure on removing illegal content takes away the opportunity to have a discussion with different parts of society about it. Counter-narratives cannot be developed in isolation by companies, but engaging individuals.
- Once companies are pushed to impose restrictions, it is very difficult to pull them back when they go too far. It is important to ensure that the balance of incentives is such that restrictions that are predictable and there are review processes that allow them to be assessed to show that they are genuinely achieving objectives of general interest.
- Frequent shortcuts are made in analysing the issues of illegal content by projecting the resources and impact of the very large online platforms onto all other hosting services.

It is crucial to empower users through digital literacy, so that they can also exercise their responsibility to protect fundamental rights.

## 4.9 Workshop on notice and action in practice, held on 31 May 2017

The workshop discussed practical aspects of the Notice and Action mechanisms employed by the stakeholders: online platforms/intermediaries as notice recipients, rights-holders as notice providers. User and consumer rights, as well as the perspective of public authorities, were also discussed.

First panel on intellectual property infringements online

The panel started with a short overview of practices in handling IP infringements presented by a company specialising in monitoring IP infringements and enforcing them on behalf of right holders:

- Platforms provide interfaces (convenient for small, but sometimes difficult for big brands).
- Closed profiles of sellers of counterfeit goods are more difficult to handle for notifiers.
- Automated monitoring is allowed by some platforms but not all.
- Many platforms have three-strike policies: profiles are blocked after three notices, but it is sometimes very easy to reopen the account.

For the representatives of the creative sector, Notice & Action (N&A) is helpful for certain types (rare infringements/ neutral sites), but not for all. Platforms should have systems to detect content that has been already notified. Speed of takedown varies from platform to platform. Trusted notifiers' programmes are helpful and should have priority. Due process needs to balanced, so as not to undermine the efficiency of the process. The problem of repeat infringers exists: 95% of notices report the same content to the same sites.

Online platforms described their N&A policy. One platform said that it takes on average six hours to take down content, but that outliers exist when human intervention is needed. They argued that intermediaries do not have access to private contractual arrangements, so they do not know who the rights-holder has authorised to make content available.

The retail community argued that retailers need to have the opportunity to be involved in the N&A process. Often rights-holders communicate only with platforms, which do not inform retailers but simply block accounts.

A representative of a civil rights association argued that it is important to make distinctions between types of content. Account should be taken of small intermediaries (who have to take down one file or the whole website). The results of a survey of small intermediaries were presented: 8 out of 10 Internet Service Providers (ISPs) did not have a procedure in place, two removed content without evaluating the claim, four decided that the court order was necessary to remove content.

An organisation representing consumers agreed that it is important to make a distinction between types of content, e.g.: sales of counterfeit goods are high and still on the rise (there is a campaign on how to identify them); most products are bought overseas.

Stakeholders agreed that dialogue is key and cooperation between both sides should be promoted. Sharing best practices developed by big platforms to take down infringing content, as well as mechanisms for sharing costs, should be considered.

Second panel on non-IP-related notices such as those concerning hate speech, and defamatory or terrorist content

The panel started with a presentation by an online news portal from a Member State in which the High Court held the service provider liable for defamatory comments posted on the news portal's online forum. The case was a prominent example of the application of the liability exemption in Directive 2000/31/EC by the Court. The presentation was followed by a discussion on the potential consequences for intermediaries and users.

A representative of the police presented their work in the area of notification of illegal/harmful content to ISP's. Cooperation in the framework of Europol was discussed.

Differences between public notices and private notices were discussed. One stakeholder argued that public authorities should play a more prominent role in identifying illegal content.

### 4.10 E-Commerce Expert Group meeting on notice and action procedures, held on the 27th April 2017

DG CONNECT convened this meeting to gather information about notice and action procedures in Member States as well as their views as to their shaping should the EU decided to harmonise them. The meeting fitted into the investigation about the need for formal notice and take down procedures that the Commission committed to undertake in its Communication "Online Platforms and the Digital Single Market, Opportunities and Challenges for Europe" COM(2016) 288 final, of 25th May 2016.

Five Member States presented the procedures they had in place addressing key questions that the Commission had identified beforehand. There was also a presentation by the Council of Europe on the relationship on these procedures and more generally, on actions aimed at removing illegal content online, with human rights. The Council of Europe referred in its presentation to the Recommendation roles and responsibilities of internet intermediaries that were then being discussed77.

In the afternoon session, Member States broke out in discrete focus groups addressing different issues each. It was a brainstorming session where views were sought and exchanged according to the Chatham House rules. Ideas put forward include:

- Core of an action and notice procedure: minimum requirements for notices should be subject to the type of content signalled by the notice as well as the notion of "expeditious action".
- Transparency requirements: participants suggested that the notice provider should receive a confirmation of receipt of this notice, as a minimum. However, too many reporting requirements might place too great a burden on small business. Type of content and the origin of the notice (i.e.: a private individual or a judge) also plays a role in deciding whether or not the content provider should be informed about the removal. There was general agreement that platforms should publish their policy on takedown and that reporting on its implementation would help authorities to assess if the system works well. General public may not need the same level of information.
- Involvement of third parties and dispute resolution: counter-notices should be allowed unless the content is manifestly illegal or public authorities order the removal. The liability exemption

77 Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries CM/Rec(2018)2, adopted by the Committee of Ministers on 7 March 2018 at the 1309 meeting of the Ministers' Deputies



www.parlament.gv.at

should protect intermediaries while they assess a counter-notice. In any event, users can always sue platforms based on their contractual relationship. For some participants, advice from public authorities is desirable. In some countries, though, they could not provide advice for fear of State censorship or exclusive attribution of powers to the Judiciary. Most of the participants had not heard about the concept of “third party flaggers” before.

### 4.11 Workshop with intermediary service providers on voluntary measures, held on 6th April 2017

DG Connect hosted a stakeholder engagement workshop to gather information from a wide range of online intermediaries about their views on voluntary measures. The stakeholders invited spanned a range of business models, including online e-commerce marketplaces, social media, review sites, collaborative economy representatives and internet service providers.

State of play:

Stakeholders present reported a wide range of relationships to the intermediary liability exemptions in Directive 2000/31/EC. Some classified themselves as "mere conduits" under Article 12 of the Directive, others saw themselves as hosting.

The majority carried out voluntary measures of different kinds. Voluntary measures reported included education of users and businesses, parental control tools, filtering using algorithms and human intervention, pre-approval of sellers, Notice and Takedown systems, cooperation with the authorities and enforcement of Terms of Service.

A significant proportion of stakeholders said that they were keen to put voluntary measures in place, even at the risk of losing their exemption from liability, because maintaining a safe environment on their platform that consumers could trust was crucial to their business model and reputation.

Attendants generally mentioned not to face significant civil litigation concerning intermediary liability at the moment. However, they reported legal uncertainty about how far they were able to apply voluntary measures without losing their exemption from liability. They also raised the question of the e-Commerce Directive being applied differently in different Member States. Some stakeholders said they had been protected by the courts as exempt from liability despite their voluntary actions; others that some MS would not apply the e-Commerce Directive's exemptions fully or correctly.

Several stakeholders raised the question of fundamental rights, and highlighted the danger of undermining these through over-removal of (legal) content. What is illegal content is not always obvious, and some participants suggested that they were uncomfortable with the fact that they were asked to make judgements about legality. Several stakeholders were resistant to the idea of being mandated to carry out policing and enforcement by the authorities.

Costs reported included developing technology such as algorithms and the cost of human resources to filter or take down illegal content; this latter ranged from a few hours of a lawyer's time per month to hundreds of employees working full time on takedown.

Suggestions for ways forward:

Participants asked for more legal clarity on the extent of voluntary measures that platforms can take without losing their exemption from legal liability; a "good Samaritan" style regime that would allow them to take more voluntary action without risking their legal status.



www.parlament.gv.at

Stakeholders said they would welcome the provision of guidance to national authorities (including courts, governments, and consumer protection and competition authorities) encouraging the harmonization of the form of notices, and the use of co-regulatory initiatives. They requested that there should be limits on the level of policing, monitoring and enforcing that platforms can be asked to do by authorities.

Some stakeholders warned that mandating too much transparency could be counterproductive, as it might allow repeat infringers to work out how to bypass new measures. They argued that to prevent this, it was important that filtering mechanisms should be allowed to remain confidential.

Several speakers emphasized that not all types of illegal content are alike, and this should be borne in mind when trying to find solutions; a one-size-fits-all approach will not be effective, and any solution needs to be future-proofed.

## 5. CONSULTATIONS SPECIFICALLY FOCUSING ON TERRORIST CONTENT

### 5.1. Feedback of Member States to the questionnaire on terrorist content online

Public authorities in Member States were consulted on possible actions to tackle terrorist content online more effectively as well as express views on the scope of the problem. For that purpose, a questionnaire was sent to Member States and Europol on 1 June 2018. The Commission received 19 responses from Member States and from Europol. The questionnaire focused on three key areas: baseline scenario and problems, possible legislative options and voluntary options.

Baseline and problem

As to **provisions in national law** in relation to removal of terrorist content for preventive purposes, 15 Member States indicated that they have "notice and action procedures“ in place, only one Member State has indicated having "duty of care provisions", while transparency rules are common in 4 MSs, and safeguards are implemented in 4 Member States.

As for the **amount of terrorist content online**, two Member States report an increase or substantial increase. Four Member States have indicated that the situation remained the same and twelve Member States have indicated that terrorist content online has decreased78 .

As to the **risk of removals and potential interference with investigation and intelligence** replies showed that this is considered **a problem**, not only for impairing an investigation, but also for reducing the chances of obtaining evidence. At the same time, some countries have indicated that the risk of that content remaining online is greater than the risk of interfering with investigations. Many countries consider it necessary that companies **report on their removals** (8), although some pointed to the large amount of information that this would represent, making it impossible for authorities to process it. Others suggest that **companies store or retain the data** to be available upon request by competent authorities (8). Two proposed to explore further cooperation between law enforcement authorities and content providers. Other suggestions included an establishment of a flagging system for content that should not be removed, as well as oversight concerning the automated means.

78 See chapter 4.12 for additional considerations provided on the amount of terrorist content, shared by Member States on 22 May 2018



www.parlament.gv.at

Most Member States also consider that there is a risk of erroneous removal of legal content, suggesting safeguards, such as temporary removal before assessment, independent oversights, appeal procedures, human-in-the-loop for automation, definition of illegal content, trusted flaggers and law enforcement referrals against illegality, etc.

Views on a regulatory approach

So as to ensure **long-term effectiveness in addressing terrorist propaganda**, eight Member States called for reinforcement through legislation, six thought the voluntary approach would ensure long-term effectiveness, while five believe that voluntary measures need to be reinforced. The main arguments ran along the following lines:

- Those in favour of legislation have highlighted that legislation would apply to more companies than the ones currently participating in the EU Internet Forum.
- Four Member States have indicated that legislation would reinforce cooperation with companies in the long term.
- Legislation would create a level playing field for companies located outside the EU, highlighting that EU-based companies generally responded better to notices/referrals.
- Legislation would set the same requirements and rules for action across the EU, thereby avoiding market fragmentation.
- Other points highlighted in favour or legislation: legislation provides legal certainty for HSPs and for users; legislation allows for an oversight of actions taken by companies, facilitates law enforcement requests.
- **As to risks associated with legislation**, Member States highlighted the burden of creating oversight and dispute resolution mechanisms, **the need to adapt measures to changing modus operandi of terrorists and evolution of technology,** the need to address companies on a global level, fundamental rights concerns with regards to one hour assessment times of referred content (if no illegality is established), hampering progress achieved under the voluntary approach so far as well as the need to further assess progress under the Recommendation.

Member States were also asked to rank which measures would be considered as necessary for an impactful legislative approach (listed in order of priority):

1. Exchanges of information (including data retention) with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material
2. General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content, complemented by self-regulation
3. Reporting obligations for companies
4. Sanctions in case of non-compliance (noting that one Member State deemed this as not necessary, whereas 9 suggest it would be very necessary)
5. Nomination of points of contacts within companies
6. Defining terrorist content
7. More explicit and detailed obligations to deploy proactive measures
8. Specific requirements to cooperate with other HSPs to avoid the dissemination across platforms

9. Specific requirements in terms of action upon referrals/notices (including time limit of one hour)
10. Compulsory safeguards
11. Transparency requirements for companies vis à vis their users
12. Clarify that companies engaged in proactive measures benefit from liability exemption
13. Establishing an external monitoring/audit mechanism for assessing compliance of companies
14. Requiring Member States to increase referral capabilities, quality criteria for referral and for referral entities in Member States to provide relevant support to companies in case of doubt about qualification a terrorist content

As to the material scope of possible legislation, most Member States favoured a comprehensive definition:

- Recruitment: 13 (68%)
- Training: 12 (63%)
- Financing: 13 (68%)
- Other: online self-radicalisation, promotion of organisations, all offences from the Directive, glorification, and provocation, facilitation and incitement, CSAM, specific definition of terrorist content, all offences of Directive and national law.

Views on a voluntary approach

When asked about a voluntary approach, Member States graded the proposed elements which should in their view be further developed within the voluntary approach in terms of necessity:

- Standardised working **arrangements** between companies, law enforcement and Europol
- Stronger commitment on specific **proactive and preventive measures**
- Establishment of **contact points**, both in companies and Member States, to facilitate referrals
- Stronger commitments by companies in terms of **internal processes and resource allocation**
- **Additional support** (e.g. by Europol) to referral capacities in Member States
- More detailed requirements on **transparency and reporting**
- requirements to companies on **safeguards** against over-removal
- More **specific objectives** for companies' actions
- Establishment of an **external audit/monitoring** mechanism (noting that a number of Member States did not deem this as necessary)

### 5.2 Survey of service providers on terrorist content

A questionnaire was shared with approximately 30 companies. Out of them, the Commission received 6 responses from both larger as well as smaller companies – thereby providing valuable insights into the views of companies exposed to terrorist content online.

The main points raised could be summed up as follows:

- In response to the statements on **whether terrorist content negatively impacted companies' users, trust, and business-models**, all agreed that it had a negative impact on their users and that it had negative to very negative impacts on their business model. Companies were split with regards to risks of litigation – two did not see it as a problem (mostly due to confidence



www.parlament.gv.at

in systems they already had in place), two expressed concern, and one expressed serious concern. Five out of six companies expressed concern at the risk of having divergent national legislation in place, with three of those expressing serious concern. Other concerns raised related to the risk to free speech with too rigid legislation. Maintaining the balance provided by the e-Commerce Directive was seen as crucial by one.

- **On reinforced voluntary measures:** Two stressed the need of continuing with the Commission's voluntary approach. A Code of Conduct was perceived by one as useful, but only if it would not be accompanied by national legislation. They also thought an MoU might be too general. One urged that any such measures should be fit for purpose, and two mentioned they should be taking into account different sizes and business models of companies. An EU Certification system for compliant platforms was seen as positive, as well as the sharing of research.
- **On supporting smaller companies:** There were suggestions of incentives to implement measures (allow more flexibility and ensure any time limits are proportionate to the size of the company). Other suggestions included making tools freely available, ensuring high quality referrals; and the fostering and exchange of best practices and information.
- **As to regulatory efforts at EU level, the following responses were received:**
    - **Definition of terrorist content** – Three companies mentioned a need for an unambiguous definition, which would not undermine the rights, freedoms, and privacy of citizens and accepted by all Member States. Two believe there is no need for such a definition as they already had adequate provisions in place in their own terms of service.
    - **Requirements regarding the companies' terms of service** – Three believe it would be unduly complicated and commercially sensitive. One mentioned their Terms of Service already require users to comply with Community Guidelines and all applicable laws. One mentioned broad guidelines for best practice could be helpful and one sees this as positive, as long as the requirements were reasonable.
    - **General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self-regulation)** – In general, it was stated there already is substantial availability of national and EU regulation, as well as voluntary action; one saw this as positive if based on platform size. Another expressed concern over issues of liability.
    - **Specific requirements in terms of action upon referral (including time limit of one hour)** – This was deemed as unworkable for smaller companies. Some mentioned it also risked leading to removal without any human assessment on the part of the company. It was proposed that this should be implemented flexibly for small companies with limited staff capacities. The risk of erroneous referrals was also highlighted, namely in connection to strict deadlines imposed, and the need to take account of context, and possible translation. One company stressed that this could have significant financial implications and could hinder some in fulfilling their core missions. One company also highlighted the risk of creating business imbalance and skewing the market in favour of the largest and most profitable companies.
    - **More explicit and detailed obligations to deploy proactive measures (including automatic detection)** – Concern was expressed that this might conflict with existing legal instruments, difficulties for smaller companies to implement such measures and ensure the necessary safeguards. Possible privacy implications; possible errors or difficulty in assessing the context were also flagged, as well as doubts about the

practicality and feasibility of such measures. One company suggested these should only be applied to services that curate user-generated content.

- **Specific requirements to cooperate with other HSPs to avoid dissemination across platforms** – Some raised risks, e.g. the possible development of cartel-like situations and urged sticking with the voluntary approach.
- **Sanctions in case of non-compliance**: A number of concerns and questions were raised in relation to the thoroughness of checks and potential conflict with the e-Commerce Directive and the liability exemption, as well as fundamental rights. Some believed that existing laws and regulations already provided for sanctions. Concerns were raised about the burden on companies and limitations of automatic detection.
- **Exchanges of information with law enforcement to limit any interference with investigations** – EU Internet Forum was assessed to provide good practices. Quality referrals would need to be ensured as well as a clarification of provisions within GDPR and those in the Recommendation. One highlighted the need to avoid conflicting jurisdictions.
- **Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)** – This was strongly supported by respondents.
- **Requirement to MS to increase referral capabilities, quality criteria for referrals and for referral entities in MS to provide relevant support to companies in case of doubt about qualification as terrorist content (e.g. through points of contact)** – No major objections were expressed, other than a call for standardisation of approach and cooperation. One highlighted that this does not need to be mandated and voluntary engagement can be effective and another warned against privatising such processes. Two mentioned that quality of referrals and referral capabilities need to be improved. One highlighted the importance of their trusted flagger programme so that referrals can be routed via dedicated queues.
- **Nomination of point of contact within companies** – This was broadly welcomed. One company stressed that this should be voluntary.
- **Reporting obligations for companies** – This was generally accepted, with one company proposing annual reports, some highlighted the need for more leniency for small companies. One stressed the need for the format to allow for flexibility. A couple of companies mentioned that they were already doing this.
- **Transparency requirements for companies vis a vis their users** – This was assessed as positive, in particular for the most abused companies.
- **Compulsory safeguards, such as the ones in the general chapter of the Recommendation** – Could be perceived as too resource-intensive, namely for SMEs. One believed that the EU should have the power to block access to platforms that are not complying with most important requirements. Two believed it should be kept on a voluntary basis. One welcomed guidance on the minimum information required to constitute a valid notice and believed it should be possible for users to dispute complaints made against them.
- **The establishment of an external audit/monitoring mechanism for assessing compliance of companies** – Two did not believe an external audit was necessary and one of these advised against such a measure. Several urged against over-complication and unnecessary burden on SMEs. Another argued that this should only apply to the most abused companies.



www.parlament.gv.at

### 5.3 Group expert meetings

**The Commission organised a workshop on the transposition of the Directive on Combating Terrorism on 27 April 2018.**

The workshop covered within one of its sessions measures against public provocation content online (Article 21), but also served as a first opportunity to receive Member States' input on added-value for further voluntary or legislative action at EU level to address terrorist content online.

The workshop was attended by representatives from 24 Member States, the EU Counter Terrorism Coordinators' Office (CTC), Council Secretariat, as well as representatives of the European Parliament, EUROPOL, and EUROJUST and the Commission (DG HOME and DG JUST).

Member States provided an update on the transposition of Article 21 into national legislation. Fifteen Member States reported to have transposed it, five have partially transposed it and five provided no answer. Preliminary considerations were shared in terms of the need for further legislative or voluntary measures.

**The Commission, within the framework of the EU Internet Forum, organised a meeting on 22 May 2018.**

The meeting was attended by 26 Member States, Council Secretariat, Europol, European Commission, and EU CTC. The objective of the session was twofold: to take stock of progress made on the voluntary approach and discuss possible options for future actions.

Member States were asked to express their views on: reenforcing the existing work under voluntary arrangements; sector-specific or horizontal legislation.

Points raised in the session:

- Despite significant progress made, not all companies have adopted proactive measures, not all have responded to the data collection exercise and insufficient insights were provided on the impact of the database of hashes. Furthermore, the sustainability of actions under voluntary measures was questioned
- Three Member States explicitly expressed the need for legislation emphasising the importance of compulsory timeframes, preventing re-appearance of removed content, and the need for legal representatives of the companies within the EU and increased transparency with independent oversight.
- Eight Member States supported a continuation of the voluntary approach and urged caution in adopting legislative measures at this time, whilst the progress under the Recommendation should still be assessed.

### 5.4 Consultation meeting with Member States to support the Impact Assessment on Terrorist Content Online - 15 June 2018.

A stakeholder consultation took place on 15 June 2018 including representatives of 19 Member States, Council, the CTC, Europol, and the Commission (SG, DG HOME, and CNECT), to discuss the scope of the problems and possible options for action with regards to terrorist content online.



www.parlament.gv.at

Member States had been asked to reply to a questionnaire sent prior to the meeting. The questionnaire focused on three key areas: Problem and baseline scenario, reinforcing voluntary action, and legislative options. The meeting served as a platform to discuss the issues raised in the questionnaire more in depth.

The Commission received 15 responses from the Member States and one set of responses from Europol (covered in the section above and below respectively).

The majority of Member States have assessed that, overall, terrorist content decreased in volume, indicating however that this related primarily to content that was easily available on the bigger platforms whereas more content was stored and dispersed across a greater number of smaller service providers. Of particular concern for several Member States is the risk of interference with investigations and the requirement for access to removed content for evidentiary purposes.

A number of Member States (6) voiced support for legislation, whilst 2 Member States strongly pleaded for pursuing the voluntary approach. Those in favour of legislation highlighted the need to have a solid legal framework setting out the duties of companies including in particular those service providers that are difficult to engage with. One Member State strongly favoured a continuation of the voluntary approach but noted that should legislation be considered, necessary safeguards were to be put in place and coherence of action taken in with other policy areas was ensured. Another Member State noted that given the progress under the voluntary approach, the decrease in terrorist material, and the short time since the adoption of the Recommendation, evidence on the need for further legislative action was lacking. Many issues required further in depth discussions.

As regards possible legislative options, the following aspects were discussed:

- As regards action upon notification, the one hour removal time was seen as essential (3 Member States) for trusted flagger referrals and possibly by restricting it to "manifestly" terrorist content, exceptions could be foreseen for smaller companies where necessary.
- On preventing dissemination of terrorist content across platforms, public-private partnerships (for sharing technological solutions) and the role of Europol was noted as critical.
- Some countries (2 Member States) favoured obligations on proactive measures , justified in the case of terrorist content
- Several Member States considered sanctions to be important.
- As regards the burden on smaller companies, it was noted that they have to be included in the scope, given that the problem is now moving away from the bigger platforms.

With regards to the voluntary approach, 2 Member States strongly supported the continuation of existing efforts highlighting that the scope of cooperation is currently much wider than obligations which could be imposed by legislation.

### 5.5 Consultations with Europol

Europol was consulted alongside the Member States and companies. It provided responses to the questionnaire sent to Member States. Europol also participated in the following meetings: 4th Workshop on Transposition of the Directive on Combating Terrorism on 27 April 2018, dedicated session of the EU Internet Forum on 22 May 2018, and the Consultation meeting with Member States to support the Impact Assessment on Terrorist Content Online on 15 June 2018.

In its responses, Europol provided insights into terrorist use of the internet, the progress achieved with companies as well as challenges they face. Europol stressed the importance of cooperation between Member States, companies and Europol, so as to streamline and better coordinate referral processes and other efforts. Measures in place, to support referral activities, were seen as an important step towards ensuring effective processes and avoiding duplication. The need for company feedback was highlighted, as well as feedback on content removed by companies as a result of their own proactive measures.

### 5.6 Additional Evidence Gathering

Additional evidence gathering has been undertaken in the context of the EU Internet Forum and the implementation of the Recommendation of Illegal Content Online, as well as academic research, which has been integrated into the relevant sections.

# Annex 3: Who is affected and how?

As the Impact Assessment report does not conclude on a consolidated preferred option, but proposes, amongst the building blocks considered under the three options, the measures assessed as most effective in tackling terrorist content online. For completeness, Annex 3 presents a cost-benefit analysis for the components of all the assessed options.

These findings are reflected in the body of the Impact Assessment especially in the section evaluating impacts, as well as in the comparison of options from an efficiency point of view.

## 1 PRACTICAL IMPLICATIONS OF THE INITIATIVE

All options considered are imposing obligations on HSPs to varying degrees, as well as requirements for Member States and Europol. **HSPs** would be required to comply with a number of obligations based on a definition of what constitutes illegal terrorist content, narrow (Option 1) or comprehensive (Options 2 and 3).

**1. Removal of terrorist content**

For removal orders: All options: **HSPs** to have the mechanisms in place to remove content within 1 hour of receiving the order.

- Option 1 and 2 : **Member States** to designate competent authorities
- Option 3: **Member States** to establish specific authorities with sufficient capacity to detect and notify terrorist content.

Harmonisation of referrals:

- Option 1 does not include referrals
- Options 2: **HSPs** to ensure appropriate action and feedback on Europol referrals.
- Option 3: **HSPs** to ensure appropriate action and provide feedback on Europol and Member State referrals.

**2. HSPs (exposed to terrorist content[79]) required to take proactive measures**:

- Options 1: **HSPs exposed to terrorist content** to carry out a standardised risk assessment (1) threat of terrorist activity, known intent and perceived attractiveness of the HSP (users/viewers, business model) (2) vulnerability (i.e. effectiveness of measures already in place) (3) identification of the level of risk involving Europol. Measures may be taken on a voluntary basis.
- Option 2: **HSPs exposed to terrorist content** to present a remedial action plan with appropriate measures proportionate to the level of risk to address vulnerabilities and reinforce effectiveness of measures in place; measures taken may include further proactive measures to prevent the re-upload of illegal terrorist content

79 The exposure to terrorist content would be determined based on objective criteria/thresholds such as inter alia the number of removal orders.



www.parlament.gv.at

- Option 3: **HSPs exposed to terrorist content** are obliged to take specific measures proportionate to the risk and where appropriate economic capacity of the company to prevent upload, use reliable technical means such as automatic detection technologies to prevent the appearance and re-appearance of new or already identified terrorist material.

**3. Europol and cooperation with Law enforcement**

- All options: **HSPs** to put in place points of contacts for receiving removal orders
- Option 2: **Member States** to inform Europol of removal orders and actions taken by HSPs
- Option 3: **Member States** may channel removal orders under EU law via Europol and HSPs to channel feedback on action taken through Europol
- Option 1 and 2: **HSPs** to report on suspected criminal offences (to address the risk of the removal of terrorist content impairing investigations and analyses)
- Option 3: **HSPs** to report on suspected criminal offences (to address the risk of the removal of terrorist content impairing investigations and analyses) and **HSPs** to preserve terrorist content for reinstatement of erroneously removed content and for law enforcement purposes.

**4. Safeguards, transparency and accountability**

- All options: **HSPs** to comply with due diligence requirements to establish safeguards against the risk of erroneous removal and ensuring the protection of fundamental rights the legislation would foresee obligations for service providers to put in place effective mechanism for the content provider to contest the company's removal decision.
- All options: **Member States** to ensure complaint procedures and judicial redress (judicial redress should be available for both service providers and content providers to appeal removal orders/notifications)
- All options: **HSPs** to provide transparency reports (publish annually transparency reports on the companies' policies and actions, to increase transparency and accountability of platforms for measures taken to detect, identify and remove illegal content)
- All options: Member States to report to the Commission on number of legal orders and referrals sent
- All options: **HSPs** to report on implementation of obligations including information on measures put in place voluntarily (including proactive measures and safeguards, to increase transparency and accountability of platforms for measures to be taken to detect, identify and remove illegal content)

**5. Enforcement**

- All options: **Member States** to establish sanction regimes under national law including designation of relevant authorities and determine rules on jurisdiction (mechanism for sanctioning service providers in case of systematic/organisational and serious non-compliance with the requirements to ensure that these measures are properly enforced)
- All options: **HSPs not established in the EU** to establish a legal representative for the EU (same objective)

**6. Additional measures**

- Development of a technical tool to facilitate cooperation across national authorities and Europol, where appropriate, as the collaboration with hosting service providers

R&D&I support for development and take-up of technological solutions.

## 2 SUMMARY OF COSTS AND BENEFITS

| *Overview of Benefits* | |
|---|---|
| ***Description*** | ***Benefits*** |
| ***Direct benefits*** | |
| For **hosting services** | Under all options, harmonised rules should counter fragmentation of the Internal Market and increase legal certainty and trust. Service providers protected against being misused for terrorist purposes. |
| For **public authorities** | Reinforced ability of competent authorities and Europol to monitor effectiveness of action taken against terrorist content online and to take appropriate measures against the dissemination of terrorist content and terrorist activity in general (notably in options 2 and 3) |
| For **internet users** | Safety of users will be improved, reducing the risk of being exposed to terrorist material and reducing the risks for individuals who may be vulnerable to recruitment to terrorism (notably in options 2 and 3) |
| ***Indirect benefits*** | |
| For **citizens and society at large** | Increased security of EU citizens and the society at large. |
| **For civil society** | Further clarity as to the role and actions taken by competent authorities and service providers. |
| For **3rd party technology providers** | Creation of a market for the development of automatic content detection, filtering and moderation technologies. |

| *Overview of costs* |
|---|

www.parlament.gv.at

With regards to the costs, some of the measures have been adjusted to take into account where appropriate, the size of the company, the possible exposure to risk (likely to be determined based on the number of removal orders) and where appropriate, the size of the company. An approximate cost on both hosting service providers and public administration is presented below taking into account the differences between the various options.

| **Measures** | | **Option 1** | | **Option 2** | | **Option 3** | |
|---|---|---|---|---|---|---|---|
| | | Hosting service providers | Public administrations | Hosting service providers | Public administrations | Hosting service providers | Public administrations |
| **Action upon removal order**<br><br>*Applicable to all hosting services, out of which an estimate of 9,700 SMEs* | Measures for 1h removal for HSPs | 0.5 – 4 FTEs for companies depending on degree of assessment needed, and whether mere technical interventions as part of normal continuity procedures can accommodate the order + small one-off costs to establish procedure | Small one off costs for adapting to new procedures | 0.5 – 4 FTEs for companies depending on degree of assessment needed, and whether mere technical interventions as part of normal continuity procedures can accommodate the order + small one-off costs to establish procedure | Small one off costs for adapting to new procedures | 0.5 – 4 FTEs for companies depending on degree of assessment needed, and whether mere technical interventions as part of normal continuity procedures can accommodate the order + small one-off costs to establish procedure | Small one off costs for adapting to new procedures |
| | Designation of competent authorities and assessing feedback from companies | | Absorbed in the baseline as there is no obligation to establish an IRU | | Absorbed in the baseline as there is no obligation to establish an IRU | | Establishment of IRUs (expected from 23 Member States who do not currently have IRUs) and running costs are estimated at an average of ~3-4FTEs + EUR 20,000 running costs<br><br>+ 3 FTE for Europol |

www.parlament.gv.at

| Measures | | Option 1 | | Option 2 | | Option 3 | |
|---|---|---|---|---|---|---|---|
| | | Hosting service providers | Public administrations | Hosting service providers | Public administrations | Hosting service providers | Public administrations |
| | | | | | | | for enhanced coordination between Member States |
| **Action upon referrals**<br><br>*Applicable to all hosting services* | Measures for removal for HSPs | None | None | absorbed in removal order costs | None | absorbed in removal order costs | None |
| **Proactive measures**<br><br>*Applicable to an estimate of 150 and up to 400 hosting services exposed to terrorist content* | Risk assessment/remedial action plan | = 3 days / year training with EUROPOL incl. risk assessment for 3 staff (technical, moderation, legal) | 1 Europol/0,5 x 5 National authority experts for assistance to companies for risk assessment | = 3 days to draft remedial action plan with 3 staff (technical, moderation, legal) | 0.5 Europol/National authority experts for assistance to companies, if need be, for remedial action plans | None | None |
| | Cooperate with Europol and Member States to reinforce effectiveness of mitigating measures | None | None | Absorbed by other costs | 0,5 FTE x 5 national authorities<br><br>1 FTE in Europol | None | None |
| | Prevent re-upload of already removed illegal terrorist content | None | None | Cost of in-house manual, semi-automatic, or automatic filtering systems to prevent re-upload + cost maintenance (for companies at high risk and according to their size) | | Cost of in-house manual, semi-automatic, or automatic filtering systems to prevent re-upload + cost maintenance | |

www.parlament.gv.at

| Measures | | Option 1 | | Option 2 | | Option 3 | |
|---|---|---|---|---|---|---|---|
| | | Hosting service providers | Public administrations | Hosting service providers | Public administrations | Hosting service providers | Public administrations |
| | Use of technical tools to detect and prevent accessibility of new terrorist content | None | None | | None | OR cost of access to a shared database of hashes + contribution to maintenance | |
| | Indirect costs | None | None | None | None | None | None |
| **Cooperation between national authorities (and HSPs) and Europol** | Points of contact for HSPs | = baseline legal staff for HSP | None | = baseline legal staff for HSP | None | = baseline legal staff for HSP | None |
| | Informing Europol of actions taken | None | = baseline + marginal additional cost for electronic information | None | = baseline + marginal additional cost for electronic information | None | = baseline + marginal additional cost for electronic information |
| **Requirement to maintain accessibility of terrorist content** for law enforcement purposes | Reporting obligation | = 0.25 FTE to 1 FTE for assessment of content to report + marginal additional cost for electronic information | Cost depending on volumes reported and authorities' policies | = 0.25 FTE to 1 FTE for assessment of content to report + marginal additional cost for electronic information | Cost depending on volumes reported and authorities' policies | = 0.25 FTE to 1 FTE for assessment of content to report + marginal additional cost for electronic information | Cost depending on volumes reported and authorities' policies |
| | Retention obligation | None | None | None | None | ~ baseline + 0.25 FTE technical staff and storage costs; GDPR compliance costs assumed to be baseline costs; costs can be higher for some | None |

www.parlament.gv.at

| Measures | | Option 1 | | Option 2 | | Option 3 | |
|---|---|---|---|---|---|---|---|
| | | Hosting service providers | Public administrations | Hosting service providers | Public administrations | Hosting service providers | Public administrations |
| | | | | | | specialised HSP depending on their business model | |
| **Safeguards** | Complaint procedures and judicial redress | ~ baseline + 0,25-1 FTE for complaint handling | None | ~ baseline + 0,25-1 FTE for complaint handling | None | ~ baseline + 0,25-1 FTE for complaint handling | None |
| | Transparency | | None | absorbed in overall system | None | absorbed in overall system | None |
| | Reporting to the Commission | ~ contained in the system costs | 0,25FTE for reporting | ~ contained in the system costs | 0,25FTE for reporting | ~ contained in the system costs | Absorbed in the IRU costs |
| **Enforcement** | Requirement to establish a legal representative (for companies established outside the EU) | ~ baseline (included e-evidence Legal Rep) + 50kEUR running costs | None | ~ baseline (included e-evidence Legal Rep) + 50kEUR running costs | None | ~ baseline (included e-evidence Legal Rep) + 50kEUR running costs | None |
| | Monitoring and sanctions | | 0,25 FTE per Member State | | 0,25 FTE per Member State | | Absorbed in the IRU costs |

| ***Overview of Benefits for supporting measures*** | |
|---|---|
| ***Description*** | ***Benefits*** |
| ***Direct benefits*** | |
| For **hosting service providers** | Research and development funding made available for additional technological tools. |
| For **public authorities** | Coordination of action leading to efficiency gains in notifying of terrorist content to HPSs EU-wide. |
| ***Indirect benefits*** | |

www.parlament.gv.at

| | |
|---|---|
| For **civil society** | Increased participation and accountability in the design of new approaches to fighting illegal content |
| For **3rd party technology providers** | Possible creation of an incentive for a market for technology solutions for content moderation at scale |

| ***Overview of costs for supporting measures*** | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | Citizens/Consumers | | Businesses | | Public administrations | |
| | | One-off | Recurrent | One-off | Recurrent | One-off | Recurrent |
| **Technology Development** | Direct costs | none | none | none | none | ~ 15 FTE for setting up and maintaining a cooperation tools (over 2 years), for Europol | ~ 5FTE for running the system |
| | Indirect costs | none | None | | | none | none |
| **Public R&D on spread of illegal content** | Direct costs | none | None | none | None | From baseline EU funding | From baseline EU funding |
| | Indirect costs | none | none | none | none | From baseline EU funding | From baseline EU funding |

www.parlament.gv.at

# Annex 4: Analytical Methods

**Quantitative assessment of policy measures**

This section describes how the costs were calculated and which assumptions were used as a basis. Administrative costs will be borne by 2 groups of stakeholders as part of this initative, namely service providers and public authorities.

**1. Public Authorities**

Costs on **Member State** public authorities were calculated based on existing examples of referral capabilities within the EU.

The continous cost of a basic capacity to detect and notify terrorist content was estimated to be at 3-4 FTEs **per year** assuming that the unit would be embbeded in an existing organisation. The cost was calculated for 23 member states as five already have a significant referral capabilities and assumed to be on average, as some Member States would go beyond and some would choose to be more minimal in the establishement of capacity.

Cost of a **removal order** was assessed to remain the same as under the current baseline. While removal orders are likely to be slightly more timeconsuming than referrals, the increase in cost would likely be off-set by the increased rates for removals.

Costs relating to designating a competent authority in Member States was assumed to be marginal, however 0.5 FTE for additional burden relating to monitoring, reporting and possible sanctioning was foreseen.

Costs relating to the possible establishement of a publicly run, high-accountability hash-sharing system can be divided into one off and recurring. **One-off** costs were assessed to be around 15 FTEs over two years for the intial development and technical investement. Recurring costs were eastimated around 5 FTEs for development, upkeep and running. Estimates of costs were based on an expert assessment taking into account the development and upkeep capacity of similar systems.

With regards to the assisting companies with the **risk assessment/remedial action plan** continous costs on **Europol** are estimated to be 1 FTE per year. In addition 1-3 FTEs cost increase was foreseen for ensuring an overview of all removal orders sent to the companies by Member State competent authorities.

**2. Hosting Service Providers**

Calculations on the costs incurred by HPs were modeled on reporting on (1) volumes of notices received or content removed, as reported in the various consultations or publicly, in transparnecy reports, (2) estimates of resources allocated by companies of different sizes and with different profiles, as reported in the various consultation exercises.



www.parlament.gv.at

- Estimates for based on lowest and highest volumes of notices reported by companies publishing a transparency report in 2017. One FTE estimated to process up to 20,000 notices a year.

- Estimate for volumes of counter-notices were based on Eurobarometer data, where 21% of the respondents whose content was taken down by an HSP reported that they had contacted the service and contested the decision. However, reported data from the few HSPs who include counter-notice results in their transparency reports shows that less than 0.003% of notices are followed-up by a counter-notice today, as per tables below:

| | 2012 | 2013 | 2014 | 2015 | 2016 | 201780 |
|---|---|---|---|---|---|---|
| **Mozilla** | - | - | - | 2 | - | - |
| **Twitter** | 5 | 16 | 31 | 148 | 516 | 313 |
| **WordPress** | - | - | 69 | 44 | 50 | 5 |
| **Tumblr** | - | - | - | 115 | 205 | - |
| **Medium** | - | - | 1 | 2 | - | - |
| **GitHub** | - | - | 17 | 62 | - | - |
| **Etsy** | - | - | 115 | 569 | 1,523 | - |

| | | | 2014 | | 2015 | | 2016 | |
|---|---|---|---|---|---|---|---|---|
| | | | **Jan-Jun** | **Jul-Dec** | **Jan-Jun** | **Jan-Jun** | **Jul-Dec** | **Jan-Jun** |
| **Twitter** | Result of DMCA notices | Tweets withheld | 30,870 | 32,462 | 47,882 | 56,971 | 79,513 | 75,869 |
| | | Media withheld | 15,088 | 17,809 | 19,181 | 22,815 | 49,298 | 86,091 |
| | Result of counter-notices | Tweets restored | 83 | 2 | 34 | 65 | 59 | 236 |
| | | Media restored | 34 | 29 | 11 | 141 | 274 | 364 |
| **Tumblr** | Result of DMCA notices | Posts removed | - | - | 77,357 | 59,766 | 61,053 | - |
| | Result of counter-notices | Posts restored | - | - | 63 | 44 | 75 | - |
| **Medium** | Content removed | | 6 | | 29 | | - | |
| | Content restored | | 1 | | 3 | | - | |

80 Latest data at the time of checking

To estimate the numbers of SMEs and other companies in scope of the broader category of HSPs, the DealRoom database was used, extracting proxies of the following categories of companies. Enterprises included are companies at seed level, receiving venture or public capital and assumed to be prone to scale-up and development.

Estimates point to a basis of over **10,500 HSPs established in Europe**, and almost 20,000 HSPs established both in Europe and in the US and Canada. **Over 90% of European companies are SMEs,** and almost half are micro-enterprises (i.e. fewer than 10 employees, turnover/balance sheet lower than 2 mil EUR). Estimates below are conservative, based on companies considered to have a high growth potential.[81]

| ***Type of company*** | **Number of companies: EU established** | **% of total SMEs** | **Number of companies: Global [82]** | **% of total SMEs** |
|---|---|---|---|---|
| *Small* | 1,427 | 15% | 2,991 | 17% |
| *Medium* | 3,874 | 40% | 6,786 | 40% |
| *Micro* | 4,388 | 45% | 7,370 | 43% |
| | | | | |
| *Total SMEs* | **9,689** | **92%** | 17,147 | 89% |
| *Total companies* | 10,522 | | 19,344 | |

81 Dealroom database

[82] EU, US, and Canada over-represented



www.parlament.gv.at

# Annex 5: Impact on fundamental rights

Chapter 6.4 of the Impact Assessment summarises the impact of the different options on fundamental rights. This analysis is presented more in detail in the present annex.

The fundamental rights considered include in particular the right to life and right to dignity, respect of private and family life and the protection of personal data (Article 7 of the Charter), freedom of expression and information (Article 11 of the Charter), and the freedom to conduct a business (Article 16 of the Charter).

Where negative impacts were identified, an assessment was made whether any limitation to the fundamental right in question would be necessary to achieve an objective of general interest recognised by the Union or to protect the rights and freedoms of others and whether such limitations would be proportionate, i.e. appropriate for attaining the objective pursued and not going beyond what is necessary to achieve it, and in particular if there is an alternative that is equally effective, but less intrusive.

## 1 Definition of terrorist content/propaganda

For the purposes of preventing dissemination of terrorist material online, a definition of terrorist propaganda would be aligned as closely as possible to the relevant provisions of the Terrorism Directive. The assessment of the content would need to account factors such as the nature and wording of the statements, the context in which the statements were made, including whether it is disseminated for educational, journalistic or research purposes, and the potential to lead to harmful consequences.

Not all statements sympathising with terrorist actions or causes are protected by article 11 of the Charter or Article 10 of the European Convention on Human Rights. The European Court on Human Rights has consistently held that speech that is incompatible with the values proclaimed and guaranteed by the Convention is not protected by Article 10 of the Convention. This notion has also been applied regarding terrorist propaganda[83]. Therefore, to the extent that terrorist content constitutes an incitement to violence and support for terrorist activity or organisations it is not protected under article 11 of the Charter in the first place.

Where the statements in question could be regarded as in principle falling under Article 10 of the Convention, the delimitation of the scope of the definition of terrorist content for the purpose of envisaged legislation at EU level takes into account the relevant case law and the justification for

83 ECHR, Application no. 24683/14 ROJ TV A/S against Denmark. The decisive point when assessing whether statements, verbal or non-verbal, are removed from the protection of Article 10 by Article 17, is whether the statements are directed against the Convention's underlying values, for example by stirring up hatred or violence, and whether by making the statement, the author attempted to rely on the Convention to engage in an activity or perform acts aimed at the destruction of the rights and freedoms laid down in it. Other examples of such speech declared by the Court as not being protected by freedom of speech under Article 10 include notably, the dissemination of the political ideas of Hizb ut-Tahrir (Hizb ut-Tahrir and Others v. Germany, No. 31098/08; Kasymakhunov and Saybatalov v Russia, No. 26261/05 and 26377/06,), incitement to discrimination, hatred and violence (Belkacem v. Belgium, No. 4367/14), or defending Sharia while calling for violence to establish (Refah Partisi (The Welfare Party) and Others v. Turkey, nos. 41340/98).



www.parlament.gv.at

interferences with the legitimate aim to protect national security, preventing crime and acts of terrorism.

Whether these statements fall already outside the scope of Article 10 of the Convention or are within the scope but interferences are justified, needs to be determined on the basis of nature and wording of the statements, the context in which the statements were made and the potential to lead to harmful consequences, among other criteria (see Stomakhin v Russia)84. The fact that material is produced by and disseminated by listed terrorist organisations in pursuit of their aims can be an indicator in this regard. Furthermore, the scope of the definition of terrorist propaganda needs to be seen in connection with the scope of obligations imposed on companies including possible sanctions in case of non-compliance.

Under Option 1, with a narrow definition of terrorist content limited to direct incitement, it can be expected that material would be easily recognised and taken down without a high risk that legal content is inadvertently affected. This is to some extent still valid under Options 2 and 3 with a definition which would also cover recruitment and training for terrorism. To the extent that allegedly terrorist material could be conflated with legitimate speech, safeguards including judicial reviews of removal orders and the possibility to issue a counter notice, as well as measures taken to mitigate the possibility of erroneous removals when deploying proactive measures, including automatized means of detecting terrorist content, will mitigate the risk that content that is protected by freedom of expression would be affected.

### 2 The need for hosting service providers to respond to removal orders within one hour

**Under all the options**, HSPs would have to **respond to removal orders from national competent authorities within 1 hour**. Under Option 1 this obligation would however only apply to material that constitutes direct incitement to commit acts of terrorism.

The risk that the 1 hour time limit for response would lead to removal of legal content is mitigated by due review process which applies to removal orders issued by a national authority, available both to the HSP as well as to the content provider. While the duty to react within 1 hour will impose a burden and costs on the HSPs, thus possibly affecting the **freedom to conduct a business**, this impact is broadly mitigated by the fact that a solid legal assessment will have been carried out by the competent authorities before issuing the removal order, which the HSP will not need to assess itself. Further cooperation across national authorities would also limit possible duplication of removal orders received by an HSP for the same content, and streamline processes in comparison with the fragmented baseline.

### 3 Action upon Europol's referrals

84 Including also (b) the capacity of the person using the hate speech to exercise influence over others (such as by virtue of being a political, religious or community leaders); (c) the nature and strength of the language used (such as whether it is provocative and direct, involves the use of misinformation, negative stereotyping and stigmatisation or otherwise capable of inciting acts of violence, intimidation, hostility or discrimination); (d) the context of the specific remarks (whether or not they are an isolated occurrence or are reaffirmed several times and whether or not they can be regarded as being counter-balanced either through others made by the same speaker or by someone else, especially in the course of a debate); (e) the medium used (whether or not it is capable of immediately bringing about a response from the audience such as at a "live" event); and (f) the nature of the audience (whether or not this had the means and inclination or susceptibility to engage in acts of violence, intimidation, hostility or discrimination)."

**Under options 2 and 3,** the HSPs would have to put in place **procedures** for Europol (option 2) as well as Member States (Option 3) referrals to be assessed as a matter of priority (Option 2). Companies would be obliged to assess the need for action, but the final decision as to whether or not to remove the content is ultimately left to the company's voluntary consideration.

As concerns **freedom of expression** it cannot be assumed that a referral based on an HSP's terms and conditions as such is strictly limited to content that is illegal. A referral is not legally binding and can therefore not be challenged in a court. However, when referrals are issued by Europol, the fact that Europol is bound to act only within its mandate (determined inter alia by the Terrorism Directive and, in particular Article 4 letter (m) in the Europol Regulation), makes it unlikely that any removal decision based on referrals would concern protected speech.

The obligation on HSPs to assess the content flagged through referrals could have a significant impact on **the freedom to conduct a business** (they would have to be prepared to assess a potentially high number of notices). This burden is alleviated by the high quality of the Europol and Member States referrals.

From the point of view of the protection of **personal data and privacy,** respect of these fundamental rights will be ensured through the observance by the hosting providers of the data protection rules, notably the GDPR, and the oversight mechanisms laid out there, as well as other specific safeguards as necessary (i.e. increased transparency requirements, information to the content provider when their content is removed, complaint mechanisms, etc.).

### 4 Requirement to take proactive measures

Under all options, the HSPs exposed to terrorist content would have an obligation, to varying degrees, to take **measures to tackle the dissemination of terrorist content through their service..** Under **option 1** it would be limited to a requirement to carry out a risk assessment, while leaving it to companies whether or not to take proactive measures. **In option 2**, the HSPs would in addition have an obligation to take appropriate and proportionate measures based on the risk assessment, while leaving the choice of the measures to the companies. Such measures could include, as appropriate, measures to prevent the dissemination on their services of terrorist content already identified. Under **option 3,** companies would be obliged to take specific proactive measures proportionate to the level of risk (without there being a requirement of a risk assessment) and resources available, including as appropriate the use of other reliable technical means (such as automated detection technologies).

Following CJEU case law85, obligations imposed by national authorities on HSPs to actively monitor all the data of each of its customers in order to prevent any future infringement were regarded as contrary to the **prohibition to impose a general monitoring obligation enshrined in Article 15 of the e-Commerce Directive**. Furthermore, the same case law underlines that in the formulation of measures adopted, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures, in particular **freedom of expression, right to personal data and the freedom to conduct a business**.

85 Cases C-70/10 (SABAM v Scarlet) and C 360/10 (SABAM v Netlog NV)



www.parlament.gv.at

In terms of **freedom to conduct a business,** the mere duty to carry out a risk assessment under option 1 will have some impact on costs for the companies. This could be alleviated where such assessments are carried out in cooperation with relevant authorities and/or Europol. **Option 2** includes a **remedial action plan and the adoption of appropriate mitigating measures.** Given that **the type of measures is limited to prevention of re-uploads taking into account the specific circumstances** of the company in question, this ensures that financial burden on the HSP in terms of costs and resources does not disproportionately affect their freedom to conduct a business. Finally, **Option 3** would have the highest impact on resources requiring companies to take a number of measures including the prevention of re-uploads as well as measures and automatic tools to detect new terrorist material. However, to ensure that the obligations are proportionate the measures would be balanced to the level of risk and available resources, in particular for micro and small companies. .

Companies who report the use of filtering technologies and automated detection claim their systems are highly effective86 in terms of removing extremist content, but do not report on the costs for developing and deploying the technology. In terms of proportionality and necessity of such measures, a number of factors should be considered. Firstly, the cost "per take down" for automatized measures compared to a removal based on a notice that require manual identification, followed by a notification at the level of the HSPs, are likely to be lower than for a take-down triggered by a notice. However, start-ups and SMEs are likely to struggle to be able to support the high initial investment costs and it cannot be ruled out that there would be an impact on new HSPs entering the market. Furthermore, in order to identify the actual context and avoid false positives (see below), automatic pre-identification should be accompanied by a "human in the loop", which increases the costs exponentially.

In respect of the impact on the **freedom of expression and information**, the key matter under consideration would be whether the requirement to take proactive measures could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communication87.

Under **Option 1,** companies would not be required to take specific proactive measures; this would be left to their discretion, following a standardised risk assessment which should incentivise companies and bring further guidance with respect to the appropriateness of proactive measures and the necessary safeguards to accompany them. Impacts on the freedom of expression and information are expected to be limited given that there is no obligation to take proactive measures. .

Under **Option 2,** the measures that companies would need to adopt, depending on the level of risk, could include appropriate measures to prevent the dissemination of known terrorist content on their services; under **Option 3,** companies would be required to take appropriate proactive measures, including by using automated detection tools. The impact on the freedom of expression and information would in such circumstances depend largely on the accuracy of such tools and how well calibrated they are in terms of avoiding false positives. It is expected that technology evolves very fast

86 Information obtained from a number of larger platforms would suggest that a large proportion (up to 80-90%) of all removals of illegal content is based on automatized means of detection rather than referrals. These figures are however likely to be considerably lower for small companies given that the development costs are high.

87 Cases C-70/10 (SABAM v Scarlet) and C 360/10 (SABAM v Netlog NV)

in this area; with recent developments pointing to a decreasing error rate for false positives, according to the developers of the technology.88.

In terms of the proportionality of the intrusion of the interference, the provision of safeguards (complaint mechanism, reversibility) and a combination of automatized detection technologies with human verifications before taking a final decision on removals would be of high importance. The impacts on the freedom of expression and information are expected to be mitigated by the inclusion of safeguards against erroneous removal of legal content.

Finally, it is noted that compared to the baseline scenario where some large companies already take such voluntary actions, the requirement of taking proactive measures combined with safeguards, transparency and reporting requirements as well as close cooperation with law enforcement and Europol establishes a **legal framework which overall strengthens the respect of freedom of expression**.

As regards **impact on data protection and privacy,** proactive automatized means of detecting illegal content could involve the identification, systematic analysis and processing of information (by automated means) connected with users of the HSPs which would affect their **right to private life and personal data.** This may also affect other individuals that are not users of the service. Any such interference would need to be appropriate, limited to what is necessary and proportionate to the objective pursued. It cannot be disputed that the public policy objective responds to a serious societal need, notably that of protecting citizens from the effects of terrorist activities, thus an objective of general interest in the sense of article 52(1) of the Charter. Safeguards as well as access to remedies for unlawful processing of the personal data along the right to access and rectify the data as per GDPR are important elements to ensure proportionality.

Similar factors as those considered in respect of freedom of information would need to be assessed as regards the impact on **protection of personal data and privacy**. The way the automated detection tools work can create interferences with the right to protection of personal data. It would thus be important to establish the risk factors that algorithms will take into account. Such risk factors as indicated by the Court89 should be non-discriminatory and should also be sufficiently specific and reliable in order to make possible to identify content which fulfils the definition of terrorist content. Profiling of users create the risk of undue processing of personal data and any profiling should be accompanied by appropriate safeguards and most importantly no decision affecting the concerned person should be taken solely on the basis of profiling without human intervention. Data protection by design shall be the guiding principle in designing any such automated tools. Transparency towards users as to the automated processing through meaningful information about the logic involved in the processing of their personal data, a right to human assessment when content is taken down and access to remedies for unlawful processing of the personal data would be important safeguards (along with other safeguards foreseen under the GDPR, such as the right to access and rectify the data).

With regards to the **right to life**, which could be positively impacted by measures to prevent terrorist attacks from materialising, all options would have a more positive impact insofar measures to remove harmful content would be combined with reporting by the hosting service providers of alleged

88 Recent reports about a UK Home Office tools and tests suggesting it can detect 94 per cent of Isis videos with a 99.99% success rate https://www.gov.uk/government/news/new-technology-revealed-to-help-fight-terrorist-content-online

89 Opinion 1/15 PNR Canada point 173

terrorist content to law enforcement authorities, allowing the authorities to pursue suspected criminal offences.

## 5 Requirement to preserve removed content

The requirement under **option 3** for **HSPs to preserve content** removed through proactive measures would have an impact on the right to data protection and privacy, as it is likely that preservation of the said content will also involve retention of the data related to the content provider (and possibly other third parties).

The right to protection of personal data and the right to privacy are not absolute rights, and necessary and proportionate limitations can be justified. The objectives of pursuing important public policy objective, notably that of preventing terrorist recruitment and grooming, preventing and disrupting terrorist activity and investigating and prosecuting terrorists, could justify the limitation of rights in question. The assessment of the necessity and proportionality of such measures will thus depend on the exact purpose, scope of the measure and safeguards. The content preserved can be used (by law) for related legal proceedings, and is limited to content which was previously assessed as terrorist content (not generally to all suspicious content) and does not concern data about all users, but only about specific users that have performed activities with a direct link to a criminal offence. Retention of content taken down by the service provider as result of their proactive measures would be justified as necessary for the legitimate purpose of ensuring the effective operation of the redress mechanisms, for the benefit of both the HSP and the content originator, subject to appropriate safeguards. While it would relate to a strong suspicion of a criminal offence been committed, it would also be justified as necessary for the legitimate purpose of avoiding that the removal interferes with ongoing investigations. At any rate, the data should be retained for no longer than is necessary for the purpose of the retention, in line with data protection rules.

In terms of impact on the right to life and right to dignity, Option 3 would have a particularly positive impact in terms of ensuring that removed terrorist content it is available for evidence purposes for competent authorities' investigations, reinforcing their capacity to combat terrorist activities.



www.parlament.gv.at

# Annex 6: Legal context at EU level

## 10. EU ACQUIS

Overview of existing laws and other measures regarding (a) single market for information society services providers, intermediary liability and notification/redress/transparency requirements, (b) terrorism.

- Directive 2000/31/EC[90]

Directive 2000/31/EC establishes a country of origin principle for the provision of information society services and prohibits Member States from restricting the freedom to provide information society services from another Member State, unless for specific reasons of general interest and under specific conditions. Service providers are bound by some transparency requirements such as disclosing their name, geographic address and contact details. In its Article 14, Directive 2000/31/EC provides the conditions under which a service provider who stores information provided by the recipient of the service, is not liable for the information stored at the request of the recipient of the service. In order for providers to benefit from this exclusion of liability, they should not have actual knowledge of the illegal activity or information and should not be aware of facts or circumstances from which the illegal activity or information is apparent; or upon obtaining such knowledge or awareness, they should act expeditiously to remove or to disable access to the information. A court or administrative authority is able to require the service provider to terminate or prevent an infringement.

According to Article 15, Member States are prohibited from imposing a general monitoring obligation on providers of hosting services with regard to the information they store. Member States are free to establish obligations for information society service providers to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

- Directive 2011/93/EU[91]

The Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, in its Article 25, obliges Member States to take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory. It also provides that Member States may take measures to block access to webpages containing or disseminating child pornography toward the Internet users within their territory, and refers to the need to provide safeguards. Such measures can take different forms (including legislative, non-legislative or judicial action) and are without prejudice to voluntary action by industry.

90 OJ L 178, 17.7.2000, p. 1
91 OJ L 335, 17.12.2011, p. 1



www.parlament.gv.at

Even though the legal term used by the Directive is ‘child pornography’, in this document the term ‘child sexual abuse material’ is preferably used (except for legal quoting), as it more faithfully reflects the nature of seriousness of the offences.

- Directive (EU) 2017/541 92

Article 21 of the Terrorism Directive requires Member States to take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence, as referred to in Article 5 that is hosted in their territory. Article 21 also stipulates that Measures of removal and blocking must be set following transparent procedures and provide adequate safeguards, in particular to ensure that those measures are limited to what is necessary and proportionate and that users are informed of the reason for those measures. Safeguards relating to removal or blocking shall also include the possibility of judicial redress. The deadline for Member States to transpose the Directive in their national legal framework is September 2018.

- Directive 2010/13/EU93

Directive 2010/13/EU assigns 'editorial responsibility' to audiovisual media services providers but clarifying that editorial responsibility does not necessarily imply any legal liability under national law for the content or the services provided. This Directive does not apply to services offered via online platforms.

- Directive 2001/29/EC94/Directive 2004/48/EC95

Recital 59 of Directive 2001/29/EC recognises that in many cases intermediaries are best placed to bring copyright infringing activities to an end. Article 9 of Directive 2004/48/EC grants the possibility for an injunction against an intermediary whose services are being used by a third party to infringe an intellectual property right.

- Regulation 2006/2004/EC96

When consumers are concerned by the content take-down, under the Consumer Protection Cooperation Regulation (2006/2004/EC) the CPC authorities have clarified that social media online platforms cannot have unlimited and discretionary powers over the user-generated content and that standard terms and conditions should clearly state the main grounds on which content can be removed and how consumers are informed about and how they can appeal the removal. The 2017 revision of the CPC Regulation (EU) 2017/239497 addresses the need to better enforce EU consumer law, especially in the fast evolving digital sphere.

- Directive 2017/2455/EU98

92 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, OJ L 88, 31.3.2017, p. 6–21.
93 OJ L 95, 15.4.2010, p. 1
94 OJ L 167, 22.6.2001, p. 10
95 OJ L 157, 30.4.2004, p. 45
96 OJ L 364, 9.12.2004, p. 1
97 Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (Text with EEA relevance).
98 OJ L 348, 29.12.2017, p. 7

Directive 2017/2455/EU added article 242a in Directive 2006/112/EC which imposes an obligation on marketplaces, platforms, and portals which facilitate the supply of goods or services to keep records of those supplies for 10 years. Those records shall be sufficiently detailed to enable the tax authorities of the Member States where those supplies are taxable to verify that VAT has been accounted for correctly.

- Regulation 2016/679/EU[99]

This Regulation is without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. The Regulation establishes obligations related to the protection of personal data which apply inter alia to providers of information society services.

- Recommendation on illegal content100

The Commission's Recommendation on measures to effectively tackle illegal content online set out **operational measures** to ensure faster detection and removal of illegal content online, to reinforce the cooperation between companies, trusted flaggers and law enforcement authorities, and to increase transparency and safeguards for citizens. The Recommendation includes general recommendations relating to all types of illegal content and a specific section on terrorist content. The Recommendation provides for (a) **Clearer 'notice and action' procedures,** according to which platforms should set out easy and transparent rules for notifying illegal content, including fast-track procedures for 'trusted flaggers'. To avoid the unintended removal of content which is not illegal, content providers should be informed about such decisions and have the opportunity to contest them; (b) **more efficient tools and proactive technologies:** platforms should set out clear notification systems for users. The Recommendation encourages platforms having proactive tools to detect and remove illegal content, in particular for terrorism content and for content which does not need contextualisation to be deemed illegal, such as child sexual abuse material or counterfeited goods; (c) s**tronger safeguards to ensure fundamental rights:** to ensure that decisions to remove content are accurate and well-founded, especially when automated tools are used, platforms are encouraged to put in place effective and appropriate safeguards, including human oversight and verification, in full respect of fundamental rights, freedom of expression and data protection rules; (d) s**pecial attention to small companies:** the industry is encouraged, through voluntary arrangements, to cooperate and share experiences, best practices and technological solutions, including tools allowing for automatic detection. This shared responsibility should particularly benefit smaller platforms with more limited resources and expertise.; (e) **closer cooperation with authorities:** if there is evidence of a serious criminal offence or a suspicion that illegal content is posing a threat to life or safety, companies should promptly inform law enforcement authorities. Member States are encouraged to establish the appropriate legal obligations.

For the protection against terrorist content online, which is recognised as a matter of utmost urgency, the Recommendation has specific provisions on the (a) **one-hour rule**: considering that terrorist content is most harmful in the first hours of its appearance online, all platforms are encouraged to remove such content within one hour from its referral as a general rule; (b) **faster detection and effective removal**: in addition to referrals, the Recommendation calls upon platforms to implement proactive measures, including automated detection, to effectively and swiftly remove or disable

99 OJ L 119, 4.5.2016, p. 1
100 C(2018)1177



www.parlament.gv.at

terrorist content and stop it from reappearing once it has been removed. To assist smaller platforms, companies should share and optimise appropriate technological tools and put in place working arrangements for better cooperation with the relevant authorities, including Europol; (c**) improved referral system**: fast-track procedures should be put in place to process referrals as quickly as possible, while Member States need to ensure they have the necessary capabilities and resources to detect, identify and refer terrorist content; (d) **regular reporting**: Member States should on a regular basis, preferably every three months, report to the Commission on referrals and their follow-up as well as on overall cooperation with companies to curb terrorist online content.

Based on the Recommendation, Member States and companies are required to submit relevant information on terrorist content within three months, and other illegal content within six months of the publication of the Recommendation.

- Communication on Tackling Illegal Content Online[101]

In September 2017, the Commission called upon platforms to step up their efforts to swiftly and proactively detect, remove and prevent the reappearance of illegal content online. Concretely, with regard to the detection and notification of illegal content, online platforms were encouraged to cooperate more closely with competent national authorities, by appointing points of contact to ensure they can be contacted rapidly to remove illegal content. To speed up detection, online platforms were encouraged to work closely with trusted flaggers, i.e. specialised entities with expert knowledge on what constitutes illegal content. Additionally, the Communication called upon platforms to establish easily accessible mechanisms to allow users to flag illegal content and to invest in automatic detection technologies. As far as effective removal is concerned, the Commission clarified that illegal content should be removed as fast as possible, and can be subject to specific timeframes, where serious harm is at stake, for instance in cases of incitement to terrorist acts. Platforms were encouraged to clearly explain to their users their content policy and issue transparency reports detailing the number and types of notices received. Internet companies were also called upon to introduce safeguards to prevent the risk of over-removal. Finally, platforms were encouraged to take measures to dissuade users from repeatedly uploading illegal content and to further use and develop automatic tools to prevent the re-appearance of previously removed content.

- Communication "A European agenda for the collaborative economy"[102]

The Communication reiterated that online platforms, as providers of information society intermediary services, are under certain conditions exempted from liability for the information they store. The Commission considers that whether or not collaborative platforms can benefit from such liability exemption will need to be established on a case-by-case basis, depending on the level of knowledge and control of the online platform in respect of the information it hosts. The mere fact that a platform also carries out certain other activities - besides providing hosting services - does not necessarily mean that that platform can no longer rely on the liability exemption in respect of its hosting services. In any case, the Communication stressed that the way in which collaborative platforms design their information society service and implement voluntary measures to tackle illegal content online remains in principle a business decision and the question of whether they benefit from the exemption from intermediary liability should always be assessed on a case-by-case basis.

101 COM(2017)288
102 COM(2016) 356 final

- Communication on tackling online disinformation[103]

The Commission called upon platforms to decisively step up their efforts to tackle online disinformation which might not be illegal per se. Following this Communication, a Code of Practice committing online platforms will be developed with the support of the Commission. The aim will be to ensure more transparency, facilitate users' assessment of content, provide easily accessible tools to report disinformation and ensure that new online services include safeguards against disinformation.

## 11. PROPOSED LEGISLATION

- Proposal for a revised Audiovisual Directive[104]

Following the agreement reached on 6 June 2018 between the Council and the European Parliament, the proposed revision of the Audio-Visual Media Services Directive (AVMSD), will apply to user-generated videos shared on platforms when providing audiovisual content is an essential functionality of the service. The proposed revised Directive does not cover text or other types of non-audiovisual content (code, links, etc.). The proposed Directive will apply to video-sharing platforms established in a Member State; according to Article 28b AVMSD a company is deemed to be established in a Member State where a parent, subsidiary or other entity of the group is established in a Member State.

The proposed AVMSD establishes an obligation for platforms to prohibit in their T&Cs the sharing of terrorist, hate speech or child sexual abuse content. The proposed Directive does not include obligations regarding the removal of content or how video-sharing platforms are to process notifications from users. However, video-sharing platforms need to have in place transparent, user-friendly internal mechanisms for the resolution of complaints (e.g. cases of disagreement over removal of content).

Member States can adopt stricter or more detailed rules (Article 28a(5)) in compliance with Articles 12-15 of Directive 2000/31/EC.

- Proposal for a Directive on copyright[105]

The draft Directive on Copyright on the Digital Single Market establishes an obligation for some online platforms to take measures to ensure the functioning of agreements concluded with right-holders or to prevent the availability on their services of protected content. At the same time, it also requires the same services providers to put in place complaints and redress mechanisms that are available to users in case of disputes over the application of the envisaged measures. Information society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users are obliged to adopt “appropriate and proportionate” measures, “such as the use of effective content recognition technologies”, to ensure the functioning of agreements concluded with right-holders or to prevent the availability of identified content.

- Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC[106]

103 COM(2018) 236 final, 26.4.2018
104 COM/2016/0287 final - 2016/0151 (COD)
105 COM/2016/0593 final - 2016/0280 (COD)
106 COM/2017/10 final - 2017/0003 (COD)

The Regulation on privacy and electronic communications is without prejudice to the liability rules of intermediary service providers in Articles 12 to 15 of Directive 2000/31/EC. The proposed regulation provides that Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in the Regulation (such as the obligation that providers of the electronic communications services may process electronic communications content only if all end-users have given their consent) where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests. Under the proposed regulation, providers of electronic communications services will establish internal procedures for responding to requests for access to end-users' electronic communications data and shall designate in writing a representative in the Union in case they are not established in the Union.

- Proposal for a Regulation on promoting fairness and transparency[107]

The proposal for a Regulation on promoting fairness and transparency for business users of online intermediation services is a co-regulatory solution addressing issues identified on online platforms and in online search engines as regards their relationship with their business users. Regarding online platforms, the regulatory part of the proposed Regulation combines a set of legally binding transparency obligations on platforms and an obligation to set up internal redress mechanisms for handling complaints by business users. The obligations envisaged by this proposal concretely refer to the obligation for clear and easily available Terms and Conditions, the obligation for the communication of the reasons for the suspension and termination of the provision of their online intermediation services to a given business user and the obligation for platforms to include in their terms and conditions a clear description of the access to personal data or other data which business users or consumers provide to online intermediation services. The providers of online intermediation services shall include in their terms and conditions all relevant information relating to the access to and functioning of their internal complaint-handling system.

These legally binding obligations would be combined with a non-binding call to industry to establish an independent mediation body for complaints. Finally, an EU observatory for emerging problems, organised around an EU expert group will also be set up to monitor emerging trends and the evolution of problems.

- Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters[108]/ Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings[109]

The scope of application of the proposed Regulation is information society services for which the storage of data is a defining component of the service provided to the user, including social networks, online marketplaces facilitating transactions between their users, and other HSPs. Following this Regulation, an authority of a Member State may order a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of data for criminal proceedings. The Directive establishes the obligation for the appointment of a legal representative in

107 COM/2018/238 final - 2018/0112 (COD)
108 COM/2018/225 final - 2018/0108 (COD)
109 COM/2018/226 final - 2018/0107 (COD)



www.parlament.gv.at

the EU who shall be held liable for non-compliance with the obligations deriving from the applicable legal framework when receiving decisions and orders.

Proposal for a Regulation laying down rules and procedures for compliance with and enforcement of Union harmonisation legislation on products110

This proposal applies (inter alia) to HSPs. According to it, market surveillance authorities will have the power to request third parties in the digital value chain to provide all the evidence, data and information necessary. Market surveillance authorities will also have the power to take temporary measures, where there are no other effective means available to prevent a serious risk, including in particular temporary measures requiring HSPs to remove, disable or restrict access to content or to suspend or restrict access to a website, service or account or requiring domain registries or registrars to put a fully qualified domain name on hold for a specific period of time.

- Proposal for a Directive amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC, Directive 2005/29/EC and Directive 2011/83/EU as regards better enforcement and modernisation of EU consumer protection rules111

Some of the best practices put forward by the Commission's Guidance on the implementation of Directive 2005/29/EC on unfair commercial practices will be made mandatory with the proposed Directive. Notably, the proposed Directive imposes transparency obligations on online marketplaces related to the transactions undertaken, the ranking of offers, whether a contract is concluded with a trader, who is responsible for ensuring consumer rights. Transparency obligations are also imposed on operators of search engines to clearly indicate when results are paid and about the main parameters determining the ranking of the results.

Proposal for a Regulation of the European Parliament and of the Council on European Crowdfunding Service Providers (ECSP) for Business112

Crowdfunding service providers as defined in this Regulation are obliged to establish and maintain effective and transparent procedures for the prompt, fair and consistent handling of complaints received from clients. Crowdfunding platforms are obliged to keep a record of all the submitted complaints and the measures taken.

110 COM(2017) 795 final, 2017/0353(COD)
111 COM/2018/0185 final - 2018/090 (COD)
112 COM(2018) 113 final, 2018/0048 (COD)

# Annex 7: Supporting analysis for legal basis

The present annex presents the evidence on the potential choice of Article 114 TFEU as a relevant legal option for the legal instrument.

Article 114 TFEU establishes that the European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.

Following well-established case-law of the CJEU113, this Article is the appropriate legal basis where there are differences between Member State provisions which are such as to obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market, and a possible legal basis for measures to prevent the emergence of future obstacles to trade resulting from differences in the way national laws have developed. Provided that the conditions for recourse to Article 114 TFEU as a legal basis are fulfilled, the EU legislature cannot be prevented from relying on that legal basis on the ground that the prosecution of other policy objectives (in that case, public health protection) is a decisive factor in the choices to be made.

Recourse to Article 114 TFEU as a legal basis does not presuppose the existence of an actual link with free movement between the Member States in every situation covered by the measure founded on that basis. As the Court has previously pointed out, to justify recourse to Article 114 TFEU as the legal basis what matters is that the measure adopted on that basis must actually be intended to improve the conditions for the establishment and functioning of the internal market114.

While Article 114 TFEU is the legal basis for measures improving the Internal Market, and usually only EU services providers can benefit from the EU Internal Market, this Article can also be used to impose obligations on **services providers established outside the territory of the EU** where their service provision affects the internal market, when this is necessary for the desired internal market goal pursued. For instance, the Regulation on Geoblocking115 or the Proposal for a Regulation on promoting fairness and transparency for business users of online intermediation services116 consider that the ultimate effect of the instrument would be undermined if the geographic scope was limited to services providers established in the EU.

Finally, Article 114 TFEU can also serve as a legal basis to impose an obligation to third country companies to **appoint a representative** within the territory of the Union, insofar as this is merely

113 See, for all, C-380/03 Germany v European Parliament and Council, judgment of 12 December 2006.

114 Ssee, to this effect, Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-4989, paragraphs 41 and 42, and Case C-101/01 Lindqvist [2003] ECR I-12971, paragraphs 40 and 41.

115 Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC: " The effects for customers and on the internal market of discriminatory treatment in connection to transactions relating to the sales of goods or the provision of services within the Union are the same, regardless of whether a trader is established in a Member State or in a third country. Therefore, and with a view to ensuring that competing traders are subject to the same requirements in this regard, this Regulation should apply equally to all traders, including online marketplaces, operating within the Union"

116 https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services: Since online intermediation services and online search engines typically have a global dimension, this Regulation should apply to providers of those services regardless of whether they are established in a Member State or outside the Union, provided that (…) business users or corporate website users are established in the Union (and) business users or corporate website users offer their goods or services to consumers located in the Union.



www.parlament.gv.at

incidental with regard to the main purpose or component of the act. This is the case, for instance, for the NIS Directive117, exclusively based on Article 114 TFEU.

In order to consider whether Article 114 TFEU constitutes an appropriate legal basis for the proposed instrument, the following chapters present the existing legal fragmentation in the field of measures to tackle terrorist content online, in particular, and in the field of notice-and-action procedures in general (all types of illegal content).

## 1. EXISTING LEGAL FRAGMENTATION IN THE FIELD OF THE FIGHT AGAINST TERRORISM ONLINE:

The EU presents a patchy legal framework as regards the possibility for national competent authorities and courts to request the takedown of illegal terrorist content, or the blocking of websites publishing such content. In the majority of the cases, the order has to stem from a jurisdictional body, but some legislations allow for an administrative order –subject to court appeal. These laws cohabit with non-regulatory practices based on the voluntary cooperation by online services providers, based on the implementation of their own terms of service.

This is reflected in the transposition of the Directive on Combatting Terrorism. Article 21 calls on Member States to put in place measures to ensure swift removal of content inciting to the commission of terrorist acts. Fifteen Member States have informed the Commission that they have already transposed it. The information about transposition measures refers to existing or amended legislation allowing a prosecutor or a court to order companies the removal of content or the blocking of content or a website. In some cases, there are time limits of 24 hour or 48 hours for companies to take action. In most cases, however, these powers can only be exercised within a criminal procedure.

In addition, in a few Member States, law enforcement authorities can issue deletion orders and an important number of Member States have established mechanisms for law enforcement authorities to refer content for the voluntary removal of companies, allowing them to achieve faster removal outside a criminal procedure. Many Member States have established some sort of voluntary framework to facilitate cooperation with large HSPs.

From interviews conducted to national law enforcement authorities,[118] it appears that, in general, national authorities welcome self-regulatory initiatives. All the replying governments seem supportive of a voluntary approach being taken by intermediaries, encompassing all types of illegal content. They prefer this self-regulatory approach to be maintained allowing industry to take the lead on tackling illegal whilst working closely with them.

At the same time, law enforcement authorities seem to miss specific provisions under national or EU legislation to tackle cross border removal, as courts and authorities' orders are territorially limited as to their scope of application. In general, the obligation to remove the illegal content is limited to the relevant national territory.

117 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union " Where a digital service provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such a digital service provider is offering services within the Union, it should be ascertained whether it is apparent that the digital service provider is planning to offer services to persons in one or more Member States."

118 ICF study.



www.parlament.gv.at

In **France**, a new act was introduced in February 2015, in the aftermath of Charlie Hebdo's attack, establishing a specific take down procedure, managed by the police (Decree n. 2015-125 of 5 February 2015). It gives to the National Police Office in charge of fighting digital crimes the power to take down (block), without a court order, the websites containing illegal contents (terrorism and child sexual abuse material). The decree n. 2015-253 of 4 March 2015 applies to direct provocation/incitement to terrorism as well as glorification of terrorism (Section 421-2-5 of the criminal code). The law imposes a deadline of 24 hours for removing the content.

Within 24 hours from receiving the list of websites, the police blocks by any means the access to the websites. Central Office for Combating Information and Communication Technology crime checks at least every quarter that the content of the offending communication service is still illegal.

In 2004, during the transposition works on the e-Commerce Directive, the French Constitutional Court[119] issued a reservation of interpretation making clear that a notification sent to a hosting services provider, without a court having pronounced itself on the illegality of the material, could not trigger the liability of the HSP, unless the content was manifestly illegal: "*These provisions [relating to the liability of the hosts] cannot have the effect of engaging the responsibility of a host who has not removed information denounced as unlawful by a third party if it does not manifest such [illegal] character or if its withdrawal has not been ordered by a judge"* . The Court considered it necessary to limit the role of web HSPs in the regulation of online content because *"the characterization of an illegal message can be tricky, even for a lawyer"*.

As a result, the Law for the Confidence of the Digital Economy (2004/575 transposing the e-Commerce Directive) ordered HSPs to put in place an easily accessible and visible device enabling anyone to bring child sexual abuse material, to their attention. They are also obliged to inform the competent public authorities promptly of any unlawful activities referred to in the preceding subparagraph which are reported to them by the recipients of their services and, on the other hand, to make public their means of combating these illegal activities. In 2014120, this was extended to material concerning terrorist acts or "apologie du terrorisme".

In **Germany**, the Act to improve Enforcement of the Law in Social Networks (Netzwerkdurchsetzungsgesetz – NetzDG) covers crimes as listed in §§ 86 (propaganda), 86a (symbols of unconstitutional organisations), 89a and 91 (preparation or encouragement of serious violent offences endangering the State, and encouraging the commission of a serious violent offence endangering the state (similar to public provocation to comments acts of terrorism)), 100a (Treasonous forgery), 111 (Public incitement to crime), 126 (Breach of the public peace by threatening to commit offences), 129 to 129b (forming criminal and terrorist organisations), 130 (incitement to hatred), 131 (Dissemination of depictions of violence), 140 (Rewarding and approving of offences), 166 (Defamation of religions, religious and ideological associations), 184b in connection with 184d (therefore only related to child sexual abuse material), 185 bis 187, 201a (mobbing, added by the amendment), 241 (Threatening the commission of a felony) or 269 (Forgery of data intended to provide proof) of the Criminal Code.

The NetzDG introduced compliance obligations for social networks when dealing with take down notifications (user complaints) concerning illegal third party content. The act is only applicable if the illegal content fulfils the elements of specific offenses of the German Criminal Code, including for

[119] Decision No 2004-496 of 10 June 2004
120 LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

example, dissemination of propaganda material of unconstitutional organisations (Section 86 StGB), preparation of a serious violent offence endangering the state (Section 89a StGB) and forming terrorist organisations (Sections 129, 129a StGB). The law requires social networks to take down or block unlawful content within 24 hours of receiving a complaint, if the content is manifestly unlawful, within 7 days in general if the content is unlawful. Systemic failures when dealing with complaints can result in fines of up to 50 million euros.

In the **United Kingdom,** there is provision in UK law for the police to issue a notice and takedown order where unlawful content is hosted in the UK. Section 3 of the Terrorism Act 2006 currently allows internet companies two working days from notification to take down content, before they are deemed to endorse it.

According to the Terrorism Act (2006):

- **Sections 1 and 2:** Make it an offence to publish a statement encouraging terrorism or to disseminate a terrorist publication. Both sections are subject to a defence if the person can show that the statement/publication did not express his views and was not "endorsed" by him.
- **Section 3:** Provides that a person is taken to have endorsed a statement, article or record when they have been served with a notice (by the police) and have not complied with this notice within 2 working days.
- **By Section 3(4):** If the person subsequently publishes the same material ("a repeat statement") there is no need for a further notice to have been served in order for the person to be found to have endorsed the statement. The person can escape liability if they can show that he has "taken every step he reasonably could to prevent a repeat statement from becoming available to the public and to ascertain whether it does" and that he was not aware of the publication of the repeat statement.
- Police Counter-Terrorism Internet Referral Unit (CTIRU) instead refers content that breaches terrorism legislation to companies for removal on a voluntary basis when content breaches companies' terms of use. To date, the UK has found this process quicker and more effective than using the current powers available.

CTIRU have also developed relationships with over 300 online platforms and have been awarded trusted flagger status with the vast majority of major social media platforms. Since it was established in 2010, the reports by the CTIRU led to the removal of over 300,000 pieces of content.

**In Austria**, both the Federal Criminal Office (*Bundeskriminalamt*) and the Federal Agency for State Protection and Counter Terrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*, „BVT") – which are under the umbrella of the Ministry of Interior – can receive complaints (Bundeskriminalamt for child sexual abuse material and sex tourism, Bundesamt für Verfassungsschutz und Terrorismusbekämpfung against national socialism reactivation) from every citizen, anonymously.

For radical Islamic videos, notices are sent to a special email hotline of Federal Agency for State Protection and Counter-Terrorism. The agency informs HSP (YouTube/Google and Facebook) with accelerated procedure whether to remove content.

**Bulgaria** passed recently the 2017 Counter-Terrorism Act, in force as of 3 January 2017. Upon detection of Internet sites which content incites terrorism or where information about perpetration of terrorism is disseminated, the Ministry of Interior ("MoI") and the State Agency on National Security

("SANS") may submit a request to the Chairperson of the Specialised Criminal Court to order all undertakings providing electronic communications networks and/or services to block access to any such Internet sites. The request has to contain information regarding the Internet site, as well as reasons for its blocking.

The Chairperson of the Specialised Criminal Court or a deputy chairperson empowered thereby shall decide upon the request within **24 hours**. The orders for blocking access to the Internet sites issued by the court are to be published immediately after their receipt on the official Internet sites of the MoI and the SANS. The service provider shall block access to the Internet sites concerned immediately after publication of the order.

The blocked Internet sites are to be checked once every three months by the MoI and the SANS, respectively. In the cases where it is established that the content inciting terrorism or disseminating information about the perpetration of terrorism has been deleted, the MoI and the SANS have to notify the authority who issued the order on blocking the access. In such cases the Chairperson of the Specialised Criminal Court or a deputy chairperson empowered thereby shall authorise access to the Internet sites concerned, notifying the MoI and the SANS within 24 hours. The authorisation is to be published again in the SANS and MoI websites according to the procedure established above.

**Lithuania** adopted the Law No. XII-1428 on Cyber Security of 11 December 2014, that sets specific requirements applicable to public electronic communication and HSPs. The law grants jurisdiction to law enforcement entities to issue mandatory orders to the service providers to suspend provision of their services, to retain data collected during provision of services, in cases when they are used for criminal activities. All **governmental** supervisory administrative bodies are broadly entitled to issue mandatory orders to cease unlawful activities within their area of competence, including violations that are committed by way of illegal internet content. Thus, it is possible for numerous supervisory authorities to issue mandatory orders to take down the information which violates the requirements of the Lithuanian laws. Takedown orders requested by right holders require **court** injunction.

In **Luxembourg** there is no statutory notice and action procedure. If the HSP does not voluntary complies with a request of removal, it must be obtained with a court order under a summary and expeditious proceeding (*astreinte*).

Criminal law seizures are possible for all indictable offences. In particular, these include terrorism (Articles 135-1 et seq. of the Criminal Code). Sections 33.5 and 66.3 of the Criminal Investigation Code authorise the deletion, and therefore the blocking, of these data on the physical carrier of the intermediary, only when a priori copy has been made, the deletion has been ordered by an investigating judge, or by the state prosecutor in the case of offences discovered during or immediately after their commission, the holding or use of the data is unlawful or poses a threat to persons or property, the physical carrier (for example, the computer or server) carrying the data is located in the Grand Duchy of Luxembourg.

The condition that a prior copy of the deleted data be made means that the latter can be reconstituted if the decision to delete is set aside by a judge in chambers or by a trial court, or in the event of a discharge or acquittal.

In **Malta,** under Article 22 of the Electronic Commerce Act, "information society service providers are required to promptly inform the public authorities competent in the matter of any alleged illegal activity undertaken or information provided by recipients of their service and shall grant to any such authority upon request information enabling the identification of recipients of their service with whom

they have storage agreements". In doing so, the providers are required to grant upon request by the said authority, information enabling the identification of recipients of their service with whom they have storage agreements.

In **the Netherlands,** there is no special authority that blocks, filters or orders removal illegal internet content. The police and public prosecutor can take down material or make it inaccessible in case of criminal content, e.g. child sexual abuse material. The NL IRU only reports (Notice and Take Down) content if it considers content to relate to recruitment for armed struggle (Article 205 of the Dutch Penal Code) or incitement to commit a (terrorist) crime (art. 132 Sr).

Article 54a of the Penal Code requires intermediaries acting as a service provider which only passes on or stores information from another person, to comply with orders of a public prosecutor to take all reasonable measures which could be demanded from it to make this information inaccessible.

Article 54a of the Penal Code seems not to provide for intermediaries acting as service providers to have an obligation to inform any authority of this information or unlawful activity.

The Dutch Code of Criminal Procedure (DCCP) has a special section for terrorist crimes. Article 126zi DCCP indicates that suspicion is not necessary, rather mere indications of terroristic crimes suffice for an investigating officer to request that an ISP provide information such as name, address, postal code, and residence. Regarding filtering, the government has indicated that this does not work adequately, since in case of terrorism unlawful content is not as evident as compared to e.g. child-pornography, resulting in a disproportionate interference with the right to freedom of speech.

The Supreme Court has interpreted that there is no possibility for a complaint under Article 552a of the Criminal Code against the order of the prosecutor's office to make data inaccessible under Article 54a Criminal Code121.

In **Poland**, the Anti-Terrorist Act of 10 June 2016 has given powers to certain administrative bodies and law enforcement agencies to order to demand takedown of content from hosting providers. In particular, its Article 32c establishes the necessary procedure, which entails a court order (Regional Court in Warsaw) on the basis of a request from the administrative authority. The blocking order stretches to a period no longer than 30 days, in order to prevent, counteract, and detect offences of a terrorist nature, as well as to prosecute their perpetrators. In urgent cases and if it can cause an event of a terrorist nature, the administrative authority can issue the order and ask at the same time the court for a confirming decision. If it is not confirmed within 5 days, the blocking shall stop. The order has to specify a description of the event of a terrorist nature with its legal qualification, if possible, and the circumstances justifying the need to block access to the specified IT data, as well as its location. The block is imposed for a period no longer than 3 months, prorrogable by court order.

In **Slovakia**, some specific rules of horizontal nature on notice-and-takedown are included in the E-Commerce Act, which is a direct transposition of the e-Commerce Directive. In 2015, Slovakia adopted the Anti-Terrorist package, including legislation which allows stay-down and blocking of webpages on the basis of court order, in cases Slovak public authorities will have suspicion that such webpages incite or facilitate terrorist activities.

121 Supreme Court, 15 April 2014, ECLI:NL:HR:2014:908.

As part of the package, police, prosecutor's offices, courts and intelligence services receive new powers in the fight against terrorism. Website operators and web domain providers are obligated – at the behest of a court warrant based on a prior request by the intelligence service – to shut down or prevent access to a web domain name where ideas encouraging or promoting terrorism, or extremism of a religious, political or other nature, are being spread.

In **Portugal** there is no specific legislation aimed at preventing and combating online terrorism and child sexual abuse material. There is the applicable general legislation, such as Law no. 109/2009 of September 15th (Law on Cybercrime) and Law no. 32/2008 of July 17th, as well as the Portuguese Criminal Procedure Code (Decree-Law no. 78/87, of February 17th), yet there are no specific procedures for these crimes.

This legislation allows for the notification of the ISP to provide the competent authorities with certain data necessary to investigate a crime committed online (e.g. data related to the source and destination of communications, date and time of communications, equipment used), the interception of communications, searches on computer systems and apprehension of data found therein, apprehension of electronic mail, as well as home searches and seizure of the objects (such as computers) used for the commission of these offences. Under the terms of Article 19 of the Law on Cybercrime, online undercover operations are permitted for the investigation of crimes committed online, which includes terrorism and child sexual abuse material.

## 2 EXISTING LEGAL FRAGMENTATION IN THE FIELD OF THE FIGHT AGAINST ILLEGAL CONTENT ONLINE (ALL TYPES OF ILLEGAL CONTENT) AND NOTICE-AND-ACTION MECHANISMS

The e-Commerce Directive[122] establishes in its Article 3 the country of origin principle, following which information society services providers have to comply with the law of the Member State where they are established. Harmonisation being only the last resort, the principle by which Member States are not allowed to restrict the provision of services from another Member State represents the cornerstone of the Single Market and is absolutely necessary to build a Digital Single Market. Following the e-Commerce Directive, restrictive measures against a given information society service provider established in a different Member State can only be allowed if they are necessary and proportionate to protect objectives of public policy, public security, public health or protection of consumers.

As a result, an online platform offering a video uploading feature, established in one EU Member State, should adapt its reporting functionalities to allow for copyright claims under the specific conditions established by law in Finland, Hungary, Lithuania, the United Kingdom, Spain, Sweden and by case-law in Belgium, the Czech Republic, Germany or Italy (and try to comply with contradicting rulings). For that purpose, it should probably hire and maintain in-house specialists and subcontract local legal experts in each and every Member State where it desires to offer its services.

122 Directive 2000/31/EU of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.



www.parlament.gv.at

### a. National legislation on notice-and-action procedures

Some Member States have enacted notice-and-action procedures applicable to hosting activities in their national legislation. This is the case in particular in Finland[123], France[124], Hungary[125], Lithuania[126], the United Kingdom[127], Spain[128], Sweden[129], and most recently in Germany[130]; Belgium and Poland[131] have expressed their interest in legislating.

**This fragmentation can be summarized as follows**:

- There are no specific rules at the EU level when it comes to notice and action procedures;
- There are some limited efforts of voluntary cooperation that led to voluntary agreements covering also notice and action procedures, which are however limited to specific areas (protection of children online; hate speech; fight against counterfeiting);
- Only a small number of Member States actually introduced regulatory frameworks on notice and action.
- While most of these did that in the legislation implementing the e-Commerce Directive (e.g. Finland, France, Hungary, Lithuania or the United Kingdom), one can also identify examples where this was done through a self-standing legal instrument (Spain).
- In most of these cases notice and action procedures apply only to the area of intellectual property rights (Hungary, Lithuania, Spain), or even only to the area of copyright and related rights (Spain). Germany has recently introduced a type of notice and action procedure for several criminal offences that constitute illegal hate speech or illegal "fake news".
- Only France, Finland, Sweden and the United Kingdom's regulations contain requirements applying to various categories of illegal content (but none to "all types of illegal content").

In France, notice-and-action procedures are limited to "manifestly illegal content"[132]; Portugal limits actual knowledge standards to "manifestly illegal information or activity". Austrian courts have consistently limited "actual knowledge" to "obvious to any non-lawyer without further investigation"

123 Act No 2002/458 on the Provision of Information Society Services (transposing the e-Commerce Directive).
124 Law No 2004-575 of the 21 June 2004 to support confidence in the digital economy
125 Act CVIII of 2001 on certain aspects of Electronic Commerce and on Information Society Services (transposing the e-Commerce Directive)
126 The decree of the Government of the Republic of Lithuania of 22 August 2007, No 881 on "*Approving the procedure on the removal of the possibility to access illegally acquired, created, modified, or used information*", which is based on the Law Nr. X-614 on information society services (transposing the e-Commerce Directive).
127 The Electronic Commerce (EC Directive) Regulations 2002 S.I. 2002/2013, which represents the national implementing measure in the United Kingdom.
128 Royal Decree 1889/2011 and Law 21/2014..
129 The Swedish Act on Act on Responsibility for Electronic Bulletin Boards
130 https://www.bundestag.de/dokumente/textarchiv/2017/kw20-de-soziale-netzwerke/505074
131 https://news4me.eu/EMM/enc?id=407829863.
132 This legislative provision follows a so called a *'réserve d'interprétation'* issued by the *Conseil constitutionnel* on 10 January 2004 in which the latter decided that HSPs can only be held liable for not acting expeditiously on content that has a "manifestly illegal" nature (see more in the notion of illegal information and activity under the national jurisprudence later in Chapter 4). These include: l'apologie des crimes contre l'humanité, l'incitation à la haine raciale, la pornographie enfantine, l'incitation à la violence, notamment l'incitation aux violences faites aux femmes, des atteintes à la dignité humaine.

*Figure 2: Existing initiatives in Member States on notice and action*

| MS | Legal act | Legislation in preparation | Illegal content covered |
|---|---|---|---|
| **BE** | None | Notice & Action (N&A) | |
| **DE** | Law on enforcement of rights in social networks (NetzDG) | | Hate speech |
| **DK** | None | | |
| **ES** | Royal Decree 1889/2011 on the functioning of the Commission for the protection of IPR – newly modified by Law No. 21/2014. | | Copyright infringement |
| **FI** | Act No 2002/458 on the Provision of Information Society Services | | Copyright infringement |
| **FR** | Law No 2004-575 of the 21 June 2004 to support confidence in the digital economy | | Only for manifestly illegal content |
| **HU** | Act CVIII of 2001 on certain aspects of Electronic Commerce and on Information Society Services | | IPR infringement |
| **IT** | AGCOM Regulations regarding Online Copyright Enforcement, 680/13/CONS, December 12, 2013 | | Copyright infringement |
| **LT** | Regulation on Denial of Access to Information which was Acquired, Created, Modified or Used Illegally, approved by the Government Resolution No. 881 on August 22, 2007 | | Horizontal |
| **PL** | None | Potentially working on a N&A initiative | |
| **PT** | Decree-Law No. 7/2004 of 7 January], Lei do Comércio Electrónico, January 7, 2004 | | out-of-court preliminary dispute settlement |
| **SE** | Act on Act on Responsibility for Electronic Bulletin Boards | | Copyright infringement, racist content |
| **UK** | Electronic Commerce Regulations S.I. 2002/2013 | | Horizontal - it establishes the requirements of a notice |

A study conducted by the **Council of Europe**[133] helps completing the picture. This comparative study in respect of filtering, blocking and take-down of illegal content on the Internet makes a distinction among the countries where there is a specific legal framework specifically aimed at regulating the internet and other digital media, including the blocking, filtering and removal of Internet content, and countries where there is no such specific framework. The Study covers all Council of Europe Member States (including the 28 EU Member States), the various typologies of illegal contents, and encompasses issues related to the freedom of expression as limitations to the filtering, blocking and takedown procedures.

Some of the preliminary conclusions relate to the following points134:

a) In some of the jurisdictions, the measures to block, filter and take-down Internet content **fail to meet the conditions of Article 10 of the ECHR**, according to which any restrictions on freedom of expression must be legal, legitimate and necessary in democratic society. In addition, there is at times at national level lack of transparency and information on blocking and filtering procedures.

133 Comparative Study on Blocking, Filtering and Takedown of Illegal Content on the Internet (2016, Council of Europe)
134 Speaking Notes of the Council of Europe's Secretary General to the 1247th meeting of the Ministers' Deputies (10 February 2016): https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c5e87.

b) The legislation at national level at times **does not define in a sufficiently precise way what is and is not acceptable online**. As a consequence, there is much room for interpretation, which can in turn lead to arbitrary blocking or removal of content.
c) In some of the Member States, the intervention to restrict content is based on vague concepts, such as “public morals” or “extremism”.
d) In general**, there is a lack of judicial oversight**. Namely, for example, when there exists a threat to the national security, public authorities can mandate the Internet Service providers to block access, which at times can pose issues from the viewpoint of due process.
e) The role of Internet Service Providers in regulating content varies a lot from Member State to Member State: in some Member States self-regulation is most developed, whereas in other Member States there are voluntary cooperation agreements with respect to certain types of content, which are entered into between the stakeholders and the public authorities.
f) The liability regimes – including those of hosts - also are **particularly fragmented**.

Country Reports are particularly relevant insofar as they discuss in-depth the liability regimes and the notice and takedown procedures in the 28 EU Member States. Finally, a study commissioned by the Commission (SMART 2016/0039) gives the complete overview in a comparative way of the different legislations as regards notice-and-action, relevant case-law and co-regulatory agreements conducted at national level.

The scenario is even more fragmented if the interpretation by **national courts** of the liability exemption rules, and in particular what constitutes "hosting", "actual knowledge", "expeditiously" or "passive role" is considered.

In **interviews with judges** from various jurisdictions across the EU, carried out in June and July 2017, the extent of the legal fragmentation in the intermediary liability regime was repeatedly highlighted. While some judges confirmed that the judiciary in their home countries had built up experience and case law allowing them to deal consistently with liability cases, another judge reported that their home judiciary lacked the detailed knowledge of law necessary to apply it consistently, and in fact different courts within the same country had made conflicting decisions on liability cases.

Similarly, judges agreed that interpretation of what constitutes an "active host" "actual knowledge" and "expeditious" action was complex and should be considered on a case by case basis; but there was little consensus on how to make such a judgement. Judges disagreed on what level of oversight of content would make a host active; on whether use of algorithms or automated processes could bring active knowledge or make a host active; and on the definition of "expeditious".

*Figure 3: Overview of national rules on notice and action procedures*

| | **Chanel for submitting notices** | **Information requirements for notice** | **Feedback to notice provider** | **Consultation of content provider** | **Criteria for determining "*expeditiously*"** | **Other procedural rules** |
|---|---|---|---|---|---|---|
| **Finland** | first to content provider, only later to hosting provider<br>one contact point for all notices | contact information<br>about illegal content<br>details of the location of the illegal material | yes | yes, after action is taken<br>possibility to upload the content | no | sanction for false notification |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **France** | easily accessible and visible notification point | contact details<br>proof of contacting content provider<br>reasons for notice (illegality) | | | | | sanction for unjustified notice |
| **Germany** | easily recognisable, directly accessible and permanently available procedure | No specific requirements (except for link to specific content) | yes | - | the user is informed about the decision (no possibility to react) | 24h for "manifestly unlawful" material<br>7 days for non-manifestly unlawful material | |
| **Hungary** | | - subject matter of the infringement<br>- contact details | yes | - | yes, after action was taken<br>- possibility of a counter-notice and upload of the content | - clear procedural timeframes for each of the actions | - 'good faith' clause |
| **Lithuania** | | - contact details<br>- information about the illegal content | | - | yes, before action is taken<br>- possibility to consult a competent authority | - clear procedural timeframes for each of the actions | |
| **Spain** | Commission on Intellectual Property | contact details<br>description of the alleged breach<br>any information substantiating illegality | yes | yes, before action is taken | | clear procedural timeframes for each of the actions | possibility of a judicial appeal |
| **Sweden** | no specific rules in place, just the possibility to notify the specific illegal content | | | | | | |
| **United Kingdom** | | - contact details<br>- information about the illegal content | | | | | |

*i. Notices or Court orders as triggering factor for actual knowledge*

When transposing the e-Commerce Directive or during its application, some Member States have limited to courts or administrative authorities the power to refer illegal content to an online platform or to trigger the platform's liability when doing so.

- In **France**, the Conseil Constitutionnel declared unconstitutional a provision of the transposition of the e-Commerce Directive and limited the liability to intermediary service providers to manifestly illegal content reported by a third party; for non-manifestly illegal content, only a Court order can trigger that liability.
- In **Italy**, Article 16 of Decree law 70/2003, which transposes Article 14 of the e-Commerce Directive, requires that the illegal material be removed only upon the order of the competent authority. Therefore, only the authority's order triggers actual knowledge. Only recently courts have admitted that actual knowledge may be acquired by a complete notice send by the person/right holder. There are legislative proposals to adapt the law to that case-law[135].
- In **Romania**, a service provider is reputed to have knowledge only if the illegal character of the information has been declared as such by a public authority136.
- In **the Netherlands**, the Gerechtshof Amsterdam established that, for establishing when a service provider "obtains actual knowledge", a mere notice by a third party of the presence of unlawful information was not sufficient137.

In the specific field of copyright and intellectual property rights, however, it has been traditionally assumed that rights holders' notifications trigger that liability. In other legal systems, like in the US' DMCA, notice-and-takedown procedures are exclusively foreseen for copyright claims. For other types of illegal content, the Fourth Circuit established a foundational and expansive interpretation of § 230 of the Communication Decency Act, by considering that "liability upon notice has a chilling effect on the freedom of Internet speech."138

In Europe, the legislators opted for a different solution, and established a conditional exemption of liability – rather than unconditional – for all types of illegal content. This opens the way to notice-and-action procedures that are not limited to copyright infringement. While usually all known online platforms provide with a reporting mechanism, a different question is whether those private reports trigger actual knowledge by the service provider and hence potential civil or criminal liability.

*ii. Minimum content of a notice*

In their **legislations or case-law**, a great number of Member States have further defined specific requirements on the content of a notice:

- In **Belgium**, courts have determined that notices must be sufficiently circumstantiated, without details on what this means in practice.[139]

- In **Bulgaria**, the New Counter-Terrorism Act 2017 establishes that the request has to contain information regarding the Internet site, as well as reasons for its blocking [reference].

135 http://documenti.camera.it/apps/emendamenti/getProposteEmendative.aspx?contenitorePortante=leg.17.eme.ac.4505&tipoSeduta=1&sedeEsame=referente&urnTestoRiferimento=urn:leg:17:4505:null:null:com:14:referente&tipoListaEmendamenti=1

136 Article 14 of the Law 365/2002.

137 Gerechtshof Amsterdam, 24 June 2004, 1689/03 KG, Lycos gegen Pessers.

138 Zeran v AOL, 129 F.3d 327 (4th Cir. 1997).

139 Antwerp Civil Court, 3 December 2009, A&M, 2010, n.2010/5-6, and President of the Brussels Court (NL), n 2011/6845/A, 2 April 2015

- In the **Czech Republic**, a notice must be sufficiently specific and identify the information that the notice alleges to be illegal. The notice should be substantiated, but does not have to prove beyond doubt that the specific information is indeed illegal. The notice may be anonymous.

- In **Finland**, the notice-and-action regime for copyright establishes the necessary content of a notice: the name and contact information of the notifying party; an itemisation of the material, for which prevention of access is requested and details of the location of the material; confirmation by the notifying party that the material is, in its sincere opinion, illegally accessible in the communications network; information concerning the fact that the notifying party has in vain submitted its request to the content provider or that the content provider could not be identified; confirmation by the notifying party that he/she is the holder of copyright or entitled to act on behalf of the holder of the right; and signature of the notifying party.

- In **France**, the law requires the notice to identify the details of the notifying party, a description of the litigious content, an accurate location of the litigious content on the hosting service, reasons for which the content should be withdrawn, mention of the law(s) that prohibit the content and a copy of the letter made to the author/editor for the deletion of the content, or circumstances that made such contact impossible.

- In **Germany**, the recent Law on Enforcement in social networks establishes that the duty to examine a notice only arises where a notice can be linked to specific content. However, according to case-law, notices must not be general, but must be concrete and clearly formulated. A recommendation to delete all content from a particular server was regarded as insufficiently precise.[140]

- In **Hungary**, a notice on copyright must contain the subject-matter of the infringement and the facts supporting the infringement; the particulars necessary for the identification of the illegal information; the proprietor's name, residence address or registered office, phone number and electronic mail address; where applicable, the proprietor's authorization fixed in a private document with full probative force or in an authentic instrument and issued to his representative for attending the "notice and take down" procedures.

- In **Ireland**, notices referring to copyright must contain (a) the name and address of the person claiming to be the owner of the copyright in the work concerned, (b) the grounds that the person requesting the removal of material has for such removal, and (c) a list of the material, which is to be removed.

- In **Italy**, courts have established different (and sometimes contradicting) requirements for a notice. While a notice needs to be sufficiently detailed (i.e. single URLs and title of the content)[141], according to other courts, there is no need for URL to substantiate a valid event that triggers the actual knowledge of the illegal content[142].

140 OLG Karlsruhe Urt. v. 14.12.2016 – 6 U 2/15, GRURRS 2016, 115437
141 Milan Court of Appeal, R.T.I. v. Yahoo! Italia, n. 29/2015; Turin Court of First instance, judgment 7 April 2017 No 1928, RG 38113/2013, Delta TV v Google and YouTube
142 Rome Court of Appeal, RTI v TMFT Enterprises LLC, judgment 8437/2016 of 27 April 2016

- In **Lithuania**, notices on copyright need to include the person's name or company legal representative, the detail of the owner of the intellectual property rights, contact data, the work covered by violated rights, the list of the illegal content that violates the intellectual property rights, a confirmation that the person is the owner or representative, a confirmation that the information referred to in the report are correct. There are also notice and action procedures for the law on the use of information, asking for identification, the information the Lithuanian law prohibits to publish, distribute or disseminate to the public, evidence-based arguments on the reasons the information referred violates the legislation and confirmation that the information referred to in the report is correct.

- In **Spain**, copyright-related notices need to contain the exact identification of the work or service, the owner of the corresponding rights and at least one location where the work or service is offered.

- In the **UK**, notices have to include the full name and address of the sender of the notice; details of the location of the information in question (not necessarily an URL); and details of the unlawful nature of the activity or information in question. However, notices on defamation need to include: e-mail address, the meaning which the complainant attributes to the statement referred to in the notice; aspects of the statement which the complainant believes are factually inaccurate; or opinions not supported by fact; confirm that the complainant does not have sufficient information and confirm whether the complainant consents to the operator providing the poster with the complainant's name; and the complainant's electronic mail address.

#### *iii. How expeditious is "expeditiously"?*

Article 14 of the e-Commerce Directive requires HSPs to act "expeditiously" upon obtaining actual knowledge or awareness of illegal content. However, the exact meaning of this term is unclear, in particular because of an absence of EU case-law and diverging national legislations and case-law:

- **France** has not defined a timeline for "expeditious action". Courts have taken opposing position as regards what should be considered "expeditious": in one case the Paris Court of First Instance did not find it proportionate to fine YouTube for acting only 5 days after illegal content had been notified. The same court fined DailyMotion €258.000 for acting on a notification after 4 days.
- In **Hungary**, the N&A system introduced by law foresees that the service provider shall take the necessary measures **within twelve hours** following receipt of the notification (for the removal of the information indicated in the notification). Such twelve-hour deadline is applicable only in case of **infringement of intellectual property rights** or personality rights of minor children, and there is no general definition for acting expeditiously. In fact, the Supreme Court, in a **defamation** case, found that a removal within 9 days was acceptable and the host benefitted of the exemption from liability[143].
- In **Belgium**, a court established that the notice must be sufficiently substantiated and the host cannot be held liable if the content was not expeditiously removed after the first notice, which

143 Supreme Court of Hungary Pfv.20248/2015/9.



www.parlament.gv.at

was lacking of essential elements. The host failed to remove the content **19 days** after the notice but the court did not find him guilty due to incompleteness of the notice.[144]

- In **Austria**, a general deadline for deleting a contribution was not established by the case-law. Rather, the circumstances of the individual case depend on the fact must be taken into account and the response time granted by the rapidity of the medium. The Supreme Court held that, in any case, a removal within **one week** period is too late[145].
- In **Poland** there is no established deadline, but a court decided that one month to remove a fake profile was excessive[146].

It can be concluded that national courts interpret "expeditiously" **on a case-by-case basis** taking into account a number of factors such as: the completeness of the notice, the complexity of the assessment of the notice, the language of the notified content or of the notice, whether the notice has been transmitted by electronic means, the necessity for the HSP to consult a public authority, the content provider, the notifier or a third party and the necessity, in the context of criminal investigations, for law enforcement authorities to assess the content or traffic to the content before action is taken.

*iv. Counter-notices*

Those Member States that have introduced in their legislation notice-and-action procedures have usually also provided for the possibility to issue counter-notices:

- In **Finland**, **Hungary** and **Lithuania**, the IPR-related notice-and-action procedure provides with the possibility to issue a counter-notice, with different deadlines (from 3 to 14 days).

- In **Germany**, the recently adopted Law of enforcement on social networks (NetzDG) does not create an automatic right to contest the notice, but it allows the social network, if it considers it necessary, to contact the user within the 7 days limit to assess the notice.

- In **Italy** and **Spain**, the administrative procedure established for copyright establishes the right for the content provider to contest the removal decision (with different deadlines).

- Even in the absence of a legally established notice-and-action procedure, in **Estonia**, **Latvia**, **Luxembourg** and **Portugal**, some administrative procedures ordering removal of content provide with this possibility.

In other Member States, the right to contest a notice has been further developed in national case-law. For instance:

- The right to contest a notice can be limited in the case of criminal proceedings. In the **Netherlands**, for instance, the Supreme Court considered that there is no possibility for a complaint under Article 552a of the Criminal Code against the order of the prosecutor's office to make data inaccessible under the Criminal Code147.

144 Antwerp Civil Court, 3 December 2009, A&M, 2010, n.2010/5-6, and President of the Brussels Court (NL), n 2011/6845/A, 2 April 2015.
145 Supreme Court, OGH 6 Ob 178/04a.
146 Judgement of Appellate Court in Wroclaw of 15 January 2010, I Aca 1202/09.
147 Judgement of 15 April 2014, ECLI:NL:HR:2014:908 (interpretation Art. 54a Sr).



www.parlament.gv.at

- In **Germany**, Courts have consistently established that the right to hear the content provider is one of the elements contained by the service providers' duty to assess the illegality of the content that was the object of a notice. This admits variations in the case of facts-substantiated notices, for which the service provider cannot reasonably be expected to know their accuracy148.

*v. Measures against abusive notices*

As it has been presented above, there are several Member States that introduced clear criteria (by law or by case-law) on the minimum content of a notice. The legislation described there shows that a high-level of detail on the content of a notice already establishes a **threshold to avoid abusive notices**.

However, some Member States have also imposed sanctions in case of abusive notices. For example:

- In **Finland**, both abusive notices and abusive counter-notices receive the same treatment: the person who gives false information be liable to compensate for the damage caused. No liability to compensate arises or it may be adjusted if the notifying party had reasonable grounds to assume that the information is correct or if the false information is only of minor significance, when taking into account the entire content of the notification or the plea149.
- In **France**, Article 6(4) of the Law 2004-575 of 21 June 2004 (LCEN) imposes a fine of € 15.000 and imprisonment up to one year in case of "false notice", a LCEN notice which presents content or an activity as illegal in order to obtain the withdrawal or to stop the diffusion, while knowing this information inaccurate.
- In **Hungary**, the Law providing for a notice-and-action procedure as regards infringements of intellectual property rights[150] establishes a "good faith clause", following which the service provider is not responsible for the removal of content if it acted in good faith.

*vi. Contentious cases: how to submit them to a third party*

In their respective legislations, some Member States have foreseen the situation where an online platform is confronted to difficult and contentious cases, where the unlawfulness of the content is not self-evident or manifest. In those cases, some national laws provide for the possibility to consult an independent third party or an administrative body:

- For instance, in **Lithuania** the service provider may request assistance to the Information Society Development Committee under the Ministry of Transport and Communications for clarifications.
- The **Portuguese** Decree Law 7/2004 transposing the e-Commerce directive provides for a dispute settlement against the removal of the content (ANACOM, the regulator, can decide on such cases: Article 18)
- In **Germany**, the law on enforcement by social networks (NetzDG) introduces an Internet Complaint Point (Internet-Beschwerdestelle), where any person can file a complaint, which will be dealt with by one of the two participating organisations according to their respective

148 See recently LG Leipzig, judgement of 19 May 2017 (05 O 661/15).
149 Section 194 of the Information Society Code
150 Act CVIII of 2001 on certain aspects of Electronic Commerce and on Information Society Services (transposing the e-Commerce Directive).



www.parlament.gv.at

areas of expertise (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V., FSM and eco Verband der deutschen Internetwirtschaft e.V.).

- In **France**, the Senate received a proposal for a law on the creation of an Ombudsman competent for the qualification of the unlawfulness of online content151. The decision of the Ombudsman, to be rendered in a 7-day deadline, would not be binding for the online platform; but in the case the platform follows it, it will benefit of an exoneration of civil or criminal liability.

151 https://www.senat.fr/leg/ppl16-151.html, of 25 November 2016.

# Annex 8: Self-regulatory efforts

## I. Introduction

The e-Commerce Directive152 requires Member States and the Commission to encourage the adoption of Codes of Conduct in order to help implement the Directive properly.

The Commission has set up a number of sectoral dialogues with stakeholders or initiated other self-regulatory/voluntary mechanisms which *inter alia* have dealt with the removal of (potentially) illegal content:153

1. **Code of Conduct on Countering Illegal Hate Speech Online** (DG JUST)
2. **EU Internet Forum** – terrorist propaganda (DG HOME)
3. **INHOPE network of hotlines** – child sexual abuse (DG CNECT)
4. **Memorandum of Understanding on the sale of Counterfeit Goods** (DG GROW)
5. **Safety of Products Sold Online** (DG JUST)
6. **Internet Sale of Food Chain Products** (DG SANTE)
7. **Dialogue with social media companies on illegal commercial practices** (DG JUST)
8. **Workshops on collaborative short-term rental accommodation services** (DG GROW)
9. **Consumer Protection Cooperation Joint Action** (DG JUST)

The above dialogues deal with different types of illegal content/ products infringing different areas of EU or national legislation (consumer law, product safety, etc.). They do not cover all types of illegal content (e.g. copyright).

There are also pending legislative proposals, which also include provisions on possible future stakeholder dialogues such as the proposed Copyright Directive and the Audio-visual Media Services Directive, recently adopted.

EU legislation for certain types of content recognises the usefulness of voluntary arrangements such as the Terrorism Directive (EU) 2017/541 (Article 21, read in conjunction with recital 22).

## II. Analysis

### 1. Participants

The participants in the dialogues depend on the type of illegal content.

As regards *ISPs/platforms*, on issues such as terrorist propaganda, hate speech, child sexual abuse material and illegal commercial practices Facebook, Twitter, and YouTube (Google) as well as Microsoft (in the first three) are the most prominent representatives, although there are also others. As regards online sales of goods, food safety, counterfeit goods, large online marketplaces (eBay, Alibaba, Amazon, Allegro etc.) are the most involved.

152 Directive 2000/31/EC

153 The dialogues under points 5, 6 and 8 are in a very early phase. DG SANTE reported on work as regards the internet Sale of Medicinal Products and Tobacco Products, however they, at least at present, do not address the procedural aspects of the removal of illegal content at EU level, hence are not relevant in the context of this exercise.



www.parlament.gv.at

Depending on the field, the *competent authorities* of the Member States (e.g. market surveillance authorities, law enforcement authorities, authorities responsible for consumer protection (CPC) or ministries) take part in the dialogues or EU agencies (such as Europol in the EU Internet Forum).

In areas related to the take-down of illegal products, the *relevant sector of the industry* is also represented, i.e. the food industry in relation to the internet sale of food chain products or the luxury industry in the MoU on counterfeit goods.

The *civil society* (consumer and/or free speech organisations) takes part in the dialogues either as active participants (e.g. INHOPE hotlines) or as observers (e.g. Code on Hate Speech). The EU Internet Forum includes representatives from the Radicalisation Awareness Network in particular as regards discussions on engagement with and support to civil society in the development of alternative and counter narratives. Their role and involvement seems to vary depending on the dialogue.

The dialogues seem to be open to other stakeholders to join or at least to apply the standards achieved therein.

**2. The procedures to tackle illegal content**

In order to benefit from the liability exemption in the e-Commerce Directive, platforms *inter alia* have to disable access to the illegal content or to remove it rapidly, once they become or are made aware of it. Such "notice and action" procedures exist or are currently under preparation in several Member States with respect to some or all types of illegal content (horizontal or specific to hate speech, IPR etc.).

***Who can send a notice?***

Among the examined dialogues, only two have established "notice and action" procedures in which stakeholders/users can send notices to the platforms. Under the MoU on Counterfeit Goods, the right owners can send notices to the platforms according to the agreed rules. Under the Code on Hate Speech, any user can send notices to the platforms which they review in less than 24 hours.

In the other dialogues, platforms agreed to act on notices of illegal content sent by authorities. In the context of the EU Internet Forum, platforms remove terrorist content on the basis of notices sent by the Europol Internet Referral Unit (IRU) as well as national IRUs. As regards the safety of products sold online, market surveillance authorities notify the platforms (such a procedure will be mentioned in the upcoming Commission Notice). Social media companies are also requested to react to the notices from authorities responsible for consumer protection (CPC authorities).

Finally, the INHOPE network's hotlines receive notices by any user (also anonymous notices). The platforms are notified either by the hotline or by the law enforcement authority, depending on the Member State.

***Are the procedures regulated in details or is it left to the platforms to establish their policies?***

The dialogues do not contain detailed rules on the procedures; platforms seem to establish their own policies. The MoU on Counterfeit Goods contain some minimum requirements and so does the Code on Hate Speech when it requires a reaction from the platform within 24 hours. Such rules may also be included in a future code of conduct on the online sales of goods. In the dialogue on illegal commercial practices, the Commission proposed some procedural rules to follow both by the competent authorities and the platforms (content of the notice, feedback by the platform, timeline etc.). Among the actions agreed under the EU Internet Forum, several specify details for referrals

including commitments to react in the shortest time possible, streamlining of referrals and feedback (including points if contact).

***Are there requirements for the content/quality of the notice? Are templates in use?***

There are a number of dialogues where such requirements or recommendations are established. The MoU on Counterfeit Goods elaborates that the notice needs to be effective and efficient, understandable, simple to process etc. It should clearly identify the relevant product. Templates are not in use. The Code on Hate Speech refers to the case law on valid notifications which indicates that the notice "should not be insufficiently precise or inadequately substantiated".

In the dialogue on illegal commercial practices, the Commission made some proposals to competent authorities on the content of the notice (description of the illegal content, justification, etc.). On product safety, there are no specific requirements but the description of the product and the justification are considered essential elements of the notice.

On terrorist propaganda, the IRU uses the templates provided by the platforms. The INHOPE network's hotlines also provide templates for reporting.

***Is there a possibility for a counter-notice by the uploader of the content?***

Counter-notice procedures are a safeguard against excessive or erroneous removal. The MoU on Counterfeit Goods allows for a counter-notice by the seller. In practice, this seems to be the case also with respect to the safety of products sold online.

There is no room for counter-notice in the case of child sexual abuse material or terrorist propaganda. The Code on Hate Speech does not address this question.

***What are the transparency requirements?***

It seems that only the MoU on Counterfeit Goods and the Code on Hate Speech contains transparency requirements. In the first case, the platforms commit to adopt, publish and enforce IPR policies, which should be clearly communicated and indicated on their sites and reflected in the contracts which they conclude with their sellers. They also commit to disclose, upon request, the identity and contact details of alleged infringers.

The Code on Hate Speech does not contain any explicit commitments but it indicates that the companies and the Commission agree to further discuss how to promote transparency. A conclusion from the second monitoring exercise is that while Facebook sends systematic feedback to users and practices differed considerably among the social media platforms.

As regards terrorist propaganda, platforms have general reporting mechanisms in place; however, not all companies provide specific terrorism-related reporting (Twitter invested in such specific transparent reporting mechanisms). Under the EU Internet Forum more specific indicators for reporting on agreed actions have been developed.

***Are there rules on bad-faith notices and repeat infringers?***

Where notices come from authorities, provisions on bad-faith abusive notices do not seem necessary. The MoU on Counterfeit Goods *inter alia* requires right owners to notify the platform in a responsible and accurate way and to avoid unjustified, unfounded and abusive notifications. In cases where it is obvious that notices are sent without exercising appropriate care, rights owners may be denied or may have only restricted access to the procedure. The Code on Hate Speech does not contain such rules.

Also, only the MoU contains rules on repeat infringers although platforms seem to have policies in place also in other areas.

***Are the specific rules on trusted flaggers?***

In the Code on Hate Speech, platforms commit to encourage provision of notices by trusted flaggers as well as to provide them support and training. On terrorist propaganda, the IRU is in itself a trusted flagger and platforms develop such networks. The MoU on Counterfeit Goods does not contain specific rules but the signatories are considered trusted flaggers.

***Do platforms have an obligation to cooperate with authorities?***

The platforms participating in the dialogue on illegal commercial practices as well as on product safety and food safety committed to provide a single email address to authorities. Under the Code on Hate Speech and the EU Internet Forum, they also committed to have a single point of contact.

The INHOPE hotlines have an obligation to cooperate with law enforcement authorities. Under the MoU on Counterfeit Goods, rights owners and platforms commit to cooperate with law enforcement authorities, where appropriate and in accordance with applicable law.

**3. Pro-active measures**

***Do platforms commit to take pro-active measures to remove illegal content?***

As regards the examined dialogues, there is such an explicit commitment in the MoU on Counterfeit Goods but not in the other cases. It does not mean however that, in some areas, platforms do not work on concrete measures, for example to avoid the reappearance of illegal content on other sites. Under the EU Internet Forum, companies were encouraged to urgently develop and use content detection and identification technology, i.e. machine learning, to find all relevant formats of new and historical terrorist content on all their services at the point of uploading and ensure robust mechanisms are in place to ensure swift decision-making and removal. Furthermore, companies were encouraged to optimise the database of hashes being developed in the context of the EU Internet Forum to feed the database with relevant content surfaced via multiple sources (flagging, automated detection, etc.) and to ensure that platforms and services are connected to the Database of Hashes.

Airbnb has also agreed to disconnect providers when offering their services beyond the number of days allowed in certain cities.

| TYPE OF CONTENT (VOLUNTARY DIALOGUE) | HOSTING SERVICES PARTICIPATING | PROACTIVE TAKEDOWN (% of the total removed content, compared to content removed following notices) | NUMBER OF NOTICES | % REMOVALS (OUT OF CONTENT NOTIFIED | SPEED |
|---|---|---|---|---|---|
| **TERRORISM (EU INTERNET FORUM)** | **Reached out to** 20 **platforms**, including**.** Facebook, YouTube, Microsoft, Twitter, Internet archive, Justpaste.it, Wordpress, snap, Soundcloud<br>**After Recommendation: Baaz, Dropbox, Mega, Userscloud, Telegram** | Varies across companies: e.g. 44**% (Q2 2018) to 83% (Q4 2017)** reported by **one SME**; 99% by Facebook in Q1 2018<br>Database of hashes used by 13 companies | For EU IRU:<br>Q4 2017**: 8,103 referrals**<br>Q1 2018**: 5,708 referrals** | For EU IRU:<br>Q4 2017: 89%<br>Q1 2018: 61%<br>(But between 96 and 100% for "big four": FB, YouTube, Microsoft and Twitter) | Proactive measures: 5 companies reported to remove content within 1h, out of which 3 companies could do it within 1 minute, using proactive measures.<br>For referrals: majority of companies not removing within one hour; nevertheless some have jumped from 0% to 66% removals within one hour or 8% to 52%. |
| **HATE SPEECH (CODE OF CONDUCT)** | **Facebook, YouTube, Twitter, Microsoft**<br>From January 2018, **Instagram, Google+**<br>After Recommendation: **Snap** expressed willingness to join | (not covered by the scope of the code) | **December 2016**: 600 notices<br><br>**June 2017**: 2575 notices<br>**January 2018**: 2982 notices | **December 2016**: 28%<br>**June 2017**: 59%<br>**January 2018**: 70 % | **December 2016**: 40% in 24h, 43% in 48h, **June 2017**: 51.4% in 24h, 20.7% in 48h, **January 2018**: 81.7% in 24h, 10% in 48h |
| **COUNTERFEIT (MOU)** | **Alibaba, Amazon, eBay, Priceminister/Rakuten, Allegro**<br>Since Recommendation, **Facebook** discussing entry | **December 2016**: notices represent 13.7% of total takedowns (86.3% due to proactive measures)<br>**June 2017**: Notices represent only 2.6% of the total takedowns (97.4% due to proactive measures) | **December 2016**: 14% fake products found<br><br>**June 2017**: 11% fake products found | Rights owners report that notices sent lead to takedown almost in 100 % of the cases. | Right owners suggest that takedown is made within few hours, not "without undue delay" |
| **CHILD SAFETY (INHOPE NETWORK)** | Cover a wide-range of hosting services | No sector-wide data available.<br>YouTube, for example, reports **over 85% of the CSAM** content taken down through automated means. | **2017:**<br>Nearly 90 000 reports submitted by internet users to the INHOPE network of hotlines[154] - excluding reports to the North American hotlines on content hosted in North America. | Nearly 100%.<br>NB: Reports from the public are previously checked by the INHOPE network of hotlines: 20% only identified as CSAM. The overall number of reports submitted to INHOPE hotlines is over 400,000 annually. | **2017**: 62% of the content identified was verified to have been taken down within 3 days from report to hotline, 17% within 4-6 days, 21% longer than 6 days. |

154 A report is equivalent to an URL; one URL may contain several images of videos

www.parlament.gv.at

# Annex 9: Terrorist content online – evidence summary

## 1. USE OF THE INTERNET FOR TERRORIST PURPOSES

Europe is currently dealing with a high threat from terrorism. In 2017, there were a total of 205 foiled, failed and completed terrorist attacks, which killed over 68 and injured over 800155. Recent attacks in Europe and beyond have revealed how terrorists are reliant on the internet in order to pursue and fulfil their objectives. Whilst Daesh currently presents the biggest threat to Europe, al-Qaeda and its affiliates also pose a threat. At the same time, the threat from the extreme right and extreme left must not be overlooked. Indeed, VOX-POL have described the extreme right online scene as 'buoyant and growing'.

Some terrorist groups have employed sophisticated media arms, dedicated to churning out large volumes of multidimensional terrorist propaganda, and disseminating it broadly and swiftly across the internet. Their purpose is to intimidate, to radicalise and to recruit, to facilitate and direct terrorist activity, and to glorify in their atrocities and try and boost support and morale. Their material includes threats and hate speech, training manuals, advice on how to obtain and import weapons, instructions on how to make bombs and how to kill, and elaborate footage showing the torture and execution of their victims. In a couple of cases, the use of live-streaming has also been deployed during the actual attack.

Such material circulates in the form of magazines, videos and photos. Whilst such material might often depict violent imagery, the violence might be toned down for the early stages of recruitment. From early 2017, Daesh has even taken to using cartoons to glorify and promote their ideology to young children. Audio lectures and sermons of extremist preachers have also proved popular. For example, the Counter Extremist Project (CEP) has documented 55 cases in which Anwar al-Awlaki's radicalizing influence was a key factor. (Awlaki was a US-Yemeni dual citizen and longtime cleric, propagandist and operative for al-Qaeda in the Arabian Peninsula (AQAP)). According to the CEP, he has also inspired countless others around the world via his online materials to join al-Qaeda, al-Shabab and Daesh. Even after his death, Awlaki's ideology and lectures continue to influence, propagandize, and incite to violence156. Similarly, sermons and audio recordings of Daesh's leader, Abu Bakr al-Baghdadi, also proved popular. Amidst his violent rhetoric, he also encouraged many to travel to the so-called Caliphate.

Availability of terrorist content online

Daesh remains the most prolific user of the internet for advancing its terrorist objectives and despite significant territorial losses, it remains active globally in both 'real world' and online settings. According to VOX-POL, official Daesh media outlets continue to circulate press releases/official claims of responsibility, photo montages, videos and infographics online. Almost 700 new items of official Daesh propaganda were produced in January 2018, a distinct uptick

155 According to Europol's Terrorism Situation and Trend Report 2018 (page 9).
156 Counter Extremism Project - https://www.counterextremism.com/extremists/anwar-al-awlaki

from the just over 300 items that appeared in October 2017, but still considerably fewer than the 1,200 items that were produced monthly throughout 2015, 2016, and early 2017.

Whilst there are only a few cases where it appears that perpetrators of terrorist attacks have been radicalised solely through the internet, terrorists' use of the internet has certainly helped to accelerate the radicalisation process. In recent years, it has been repeatedly witnessed how terrorists have used the internet to groom and recruit, and more recently, to provide instructions on targets and how to inflict maximum carnage. Both Daesh (*Rumiyah* and previously *Dabiq)* and AQAP (*Inspire)* have used their online magazines to inspire their supporters to carry out attacks wherever they may live and provide attack options. These magazines can still be found online and feature articles advising how to conduct attacks using vehicles, knives or homemade explosives. Semi-official and fan content can be very specific as regards preferred targets, down to encouraging the targeting of named individuals. According to research published by VOX-POL in 2017, using a unique data-set of 223 convicted UK-based terrorists, "a third (32%) prepared for their attacks by using online resources". "More than half (54%) of all actors used the internet to learn about some aspect of their intended activity", a figure which has increased over time up to 76%[157], which could be an indication of increased use of the internet by to-be terrorists or of increased availability of terrorist material online. For instance, in Denmark, a teenage girl was found guilty of attempted terrorism for having tried to make bombs to be used in terrorist attacks against her own former local school and against a Jewish school in Copenhagen. The girl, who lived in a village in the countryside, became radicalised via the internet and chat contacts in just a few months after having converted to Islam158. In the aftermath of attacks, terrorist groups such as Daesh glorify in their atrocities and urge others to follow suit. In a couple of cases, the use of 'live-streaming' during the attack by the perpetrators to further terrorise their victims and the general public has been witnessed.

Despite the degradation in output, a massive archive of content remains accessible across a diversity of online spaces. As VOX-POL indicated in its Review of 2017, whilst Daesh's presence in the physical world is in decline and this is presently also reflected in a decline in online media output, they maintain a diffuse but still robust online presence, able to influence disaffected people globally to act on their behalf. With the collapse of the so-called Caliphate, their narrative has turned to one of victimhood and encouraging attacks, using motivational and instructional material online. There has also been an increase in the amount of user generated content, produced by Daesh supporters or what Daesh themselves term *munasirun (*Arabic for helper or volunteer). At the same time, media releases by al-Qaeda and its affiliates also attempt to inspire others and advocate attacks against western targets.

Distribution patterns of terrorist content online

Daesh content has moved in the last couple of years from open platforms, such as Twitter, to closed Arabic-language messaging channels on communication services such as Telegram. This is confirmed by academics highlighting that Telegram is as yet a lower profile platform than Twitter – and obviously also Facebook – with a smaller user base and higher barriers to entry. Whilst Daesh's reach via Telegram is less than it was on Twitter, the echo chamber effect may be greater as the 'owners' of Telegram channels and groups have much greater control over who joins and contributes to these than on Twitter.

157 Terrorist Use of the Internet by the Numbers, P. Gilles at al, https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9133.12249
158 Europol TE-SAT report 2018

There is also indication that the material in question is moving to marginal hosting services, often established outside the EU159. In terms of other online platforms currently in use by Daesh and their supporters, there is a heavy reliance by the latter on content hosting sites, including a variety of Google sites such as Drive, Photos, etc. and a variety of other similar sites (e.g. Justpaste.it, Archive.org, Dropbox, etc.). In addition to hosting sites, video sharing platforms remain an important feature of Daesh's online ecology, with – also Google-owned – YouTube being the preferred such platform. According to VOX-POL, Daesh and its supporters rely on hosting sites to act as back-up 'drives' that can be resorted to when content is deleted from higher profile online spaces. Most content upload sites are not searchable (e.g. by Google) and their content can therefore only be accessed by possession of dedicated URLs.

Terrorist groups are increasingly being forced to resort to smaller, less resilient platforms, where their content has a better chance of survival. When the EU IRU was first established in 2015, only 7% of its referrals were to micro, small and unregistered companies. Three years on, this category now accounts for 68% of Europol's referrals.

While the general decrease in Daesh production is well accounted for, the trend is not necessarily stable over time, as the Daesh propaganda strategy and resources have shown fluctuations in the past, according to experts160. According to Europol161, by 2017, over 150 social media platforms were identified as being abused by terrorists for propaganda dissemination. File sharing sites are used to store and disseminate terrorist content, messaging and bot services advertise links to such content and social media aggregators store and stream content to other social media platforms. According to Europol, industry and law enforcement action have resulted in a reduction of the terrorist abuse of mainstream platforms such as Facebook, Twitter and YouTube, but similar progress has yet to be made with start-up social media and companies with limited resources. Most terrorist activity concerns the surface web. Some terrorist activity however can also be found on the Darknet. This mostly relates to fundraising campaigns, the use of illicit markets and further advertisement of propaganda hosted on mainstream social media.

Research has also shown however that companies' disruption efforts might remain heavily focused towards Daesh. Research by VOX-POL showed that disruption of Hayat Tahrir al-Sham (HTS) on Twitter was considerably lower than for Daesh supporters. For example, between January 2017 and March 2018, 77% of pro-HTS accounts remained unsuspended compared to just 6% of those accounts belonging to Daesh supporters. The median age of these un-suspended accounts was 369 days for pro-HTS, which is much higher than for pro-Daesh accounts.

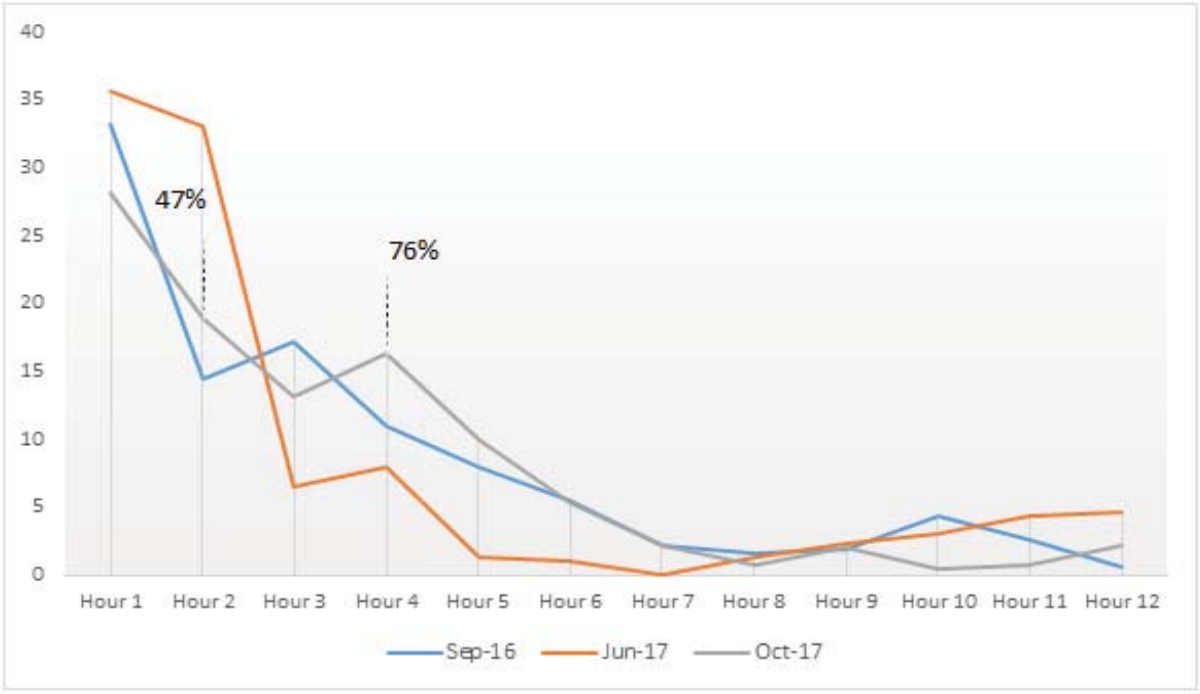
Speed of dissemination

Analysis by the UK Home Office assesses that Daesh supporters used more than 400 unique online platforms to push out their material in 2017, highlighting the importance of technology that can be applied across different platforms. Previous research has found the majority of links to Daesh propaganda are disseminated within 2 hours of release, while a third of all links are disseminated within the first hour. Their research also shows 145 new platforms from July 2017 until the end of the year had not been used before.

159 EUROPOL, *ibid.*, p29

160 Ch. WINTER, H J. INGRAM, 'Terror, Online and Off : Recent trends in Islamic State Propaganda Operations, at https://warontherocks.com/2018/03/terror-online-and-off-recent-trends-in-islamic-state-propaganda-operations/ March 2018 (accessed 15 June 2018)

161 TE-SAT 2018 https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report




How will the problem evolve?

It should be expected that terrorist groups will remain committed to the internet to advance their objectives, despite potential set-backs offline. As highlighted by the Policy Exchange in The New Netwar, 'the internet functions as another front on which they engage – one that often grows in importance as their 'real world' presence is diminished'. Whilst the likes of Daesh and other well-known terrorist groups might be forced onto the smaller platforms, they are likely to remain wedded to the larger platforms due to their wider reach. It should therefore be expect that they will continue to find innovative ways of re-establishing or increasing their presence on their larger platforms whilst in parallel being forced to resort to smaller platforms.

Since the establishment of the EU Internet Forum, there has been a growing willingness by the major tech companies to make their platforms more hostile to terrorists' exploitation. This is supported by VOX-POL research which highlighted somewhat of a turning point in 2017 as regards developments in tackling violent extremism and terrorism online, with major tech companies displaying an increased willingness to take down certain content.

## 2. WHAT HAS BEEN ACHIEVED UNDER THE EU INTERNET FORUM AND THE RECOMMENDATION ON ILLEGAL CONTENT ONLINE

In April 2015, the European Commission announced in the European Agenda on Security, the establishment of an EU Internet Forum in order to bring together the internet industry and Member States, as well as other key players such as Europol, the Radicalisation Awareness Network and the European Strategic Communications Network, in order to improve co-operation in tackling this problem and protect EU citizens – particularly EU online users. The EU Security Union Progress Reports have provided regular updates on progress and developments.

The Forum has engaged with over 20 companies and has focused its work on two key objectives: to reduce accessibility to terrorist content online and to empower civil society partners to increase the volume of effective alternative narratives online. It is the first objective which is relevant to this Impact Assessment, and a number of measures have been developed since 2015.

Firstly, Europol established an EU Internet Referral Unit in 2015 to actively scan the internet for terrorist content and then refer it to the host platform, accompanied by an assessment by Europol as to how the content is perceived as terrorism. This is a voluntary arrangement, whereby Europol refers in accordance with the company's terms and conditions. Over 50,000 decisions for referrals across over 80 platforms in more than 10 languages have been made since 2015.

It is clear that the vast majority of companies are still not in a position to be able to respond to referrals within one hour in a sustained manner – regardless of the size of the platform. The EU IRU's capability has increased significantly over the course of three years, and it is working closely with those Member States who also set up IRUs with a view to improving and streamlining the referrals process, with the establishment of tools facilitating the coordination of efforts. The number of IRUs has steadily risen to 5 and in the absence of additional action, this number is expected to increase further. With regards to removal success rates for referrals, these fluctuate from reporting period to reporting period depending on referral priorities. In the case of the EU IRU the success rates have moved between 89% (in Q4 2017) to 63% (in Q2 2018). With regards to speed of removals, in some cases improvements can be seen in terms of speeding up turn-around times for law enforcement referrals by companies, nevertheless it is clear that the vast majority of companies are still not in a position to be able to respond to referrals within one hour in a sustained manner – whether larger or smaller platforms. Furthermore, full systematic feedback mechanisms on referrals are not yet in place, although Member States do acknowledge receiving receipts and some confirmation of action from several companies.

Whilst referrals are an important element of the response, it has become clear that referrals alone will not be able to achieve the necessary impact – particularly with regards to volume and speed of response. For example, it might be a matter of hours, if not days, before IRUs might find a certain piece of content on a platform. By contrast, some of those companies using automated detection claim that content can be identified within a matter of minutes or less. Furthermore, where companies are using automated detection, referrals only seem to amount to a very small percentage of the total amount of terrorist content removed, whilst acknowledging the importance of expertise provided by the IRU referrals to companies. With this in mind, the EU Internet Forum has therefore encouraged companies to make full use of their technical and innovative capability to develop tools which can quickly identify illegal terrorist content – ideally at the point of upload – with a view to assessing it for quick action – acknowledging the importance of human assessment to avoid erroneous removals. Whilst in 2015, few companies had this capability in place, it is now understood that at least 17 companies are using some form of technology to avoid hosting illegal terrorist content or to ensure that it is identified and removed as swiftly as possible. Further to Forum meetings and bilateral outreach, more companies have indicated that they might follow suit.

Thirdly, to address the problem of the swift dissemination of terrorist content across platforms, as well as to address the re-uploading of removed terrorist content, a consortium of four companies committed at the end of 2016 to develop a Database of Hashes. The platform was implemented in 2017, and has expanded to a consortium of 13 companies with a database of over 80,000 distinct hashes of terrorist videos and images. This important tool continues to be refined and extended to



www.parlament.gv.at

additional companies. Other companies have also established tools to allow for proactive sharing of terrorist content, such as Twitter's URL database, available to 9 companies.

Academic research underpins the EU Internet Forum and helps ensure that Members of the Forum stay up to speed on how terrorists' behaviour is evolving online and Europol has established an Academic Advisory board which ensures that operational partners can keep abreast of the problem. As additional companies are brought into the Forum, it is hoped that more companies will benefit from this research and enhance their knowledge of how terrorists are or might choose to exploit their platforms.

Following the Recommendation on Illegal Content in March 2018, the Forum developed a set of indicators which are now forming part of regular reports from Members of the Forum in order to enhance collective understanding of the level of effort being applied to reduce accessibility to illegal terrorist content online. Some 14 companies have responded to the first request for reporting as well as to the second request., highlighting that not all companies addressed (33 in total) provided transparent reporting on the recommendation on illegal content online.

# Annex 10: Available technologies for detection and takedown of illegal content

A range of technologies are increasingly used to curate content accessible online, with varying levels of performance and accuracy. Some are used to identify duplicates of content previously identified as illegal, others serve as an automated flag for suspicious content or activities.

Two of the key benefits of such technologies are their ability to identify far larger quantities of harmful material than human flaggers and to identify it incredibly quickly. For example, YouTube, in its reporting for Quarter 2 in 2018, reports that between April-June 2018 alone, of the almost 8 million videos it removed, almost 7 million were removed as a result of automated flagging alone. Furthermore, 76.5% of that content was removed before there were any views162.

For those companies which have deployed such technologies in relation to terrorist content, they have seen a dramatic reduction in the amount of terrorist content hosted on their sites. This has frustrated terrorists' efforts and caused them to move – albeit reluctantly – to other more vulnerable platforms163.

## 1. FILTERING TECHNOLOGIES

### b. How they work

Filtering algorithms are based on less complex, and more mature technology than those used for identifying potentially illegal content. They are based on a two-phased process: first, assigning a unique identifier (a non-cryptographic hash) to one specific file, previously judged as illegal by a human, and sometimes by a court decision, and indexing the identifier in a database; second, when a new file is uploaded, a similar hash is generated and compared to the database. If the identifier is found, then the content is taken down. Importantly, deployment of such technology assumes that the file is illegal in itself, under all circumstances, regardless of context of use, as it is based on the simple identification of specific files.

Depending on the complexity of the identifier, the accuracy of such algorithms varies considerably. Precursors of currently used filtering technologies were based on the metadata of the file, in particular for flagging misuse of copyrighted content. These methods are generally not fully reliable and produce 'false negatives' – i.e. fail to infringing content.

More advanced methods include hashing where a unique hash is created on the basis of the encoding of the content. This method is effective when the re-upload of the identical file is

162 Q2 2018 of YouTube Transparency report.
163 http://www.jihadica.com/come-back-to-twitter/

concerned but the slightest change to the file – from its length to its file format – will generate a completely different hash.

A third generation of identifiers allows to 'fingerprint' a file on the basis of the content itself (e.g. patterns in frequencies for audio files, movement in videos). Closer to the complexity of recognition algorithms, fingerprinting technologies are also more sensitive than regular hashing to changes made to the content. While fingerprinting will more accurately find re-uploaded content and would lead to fewer 'false negatives', it can also present a certain risk of 'false positives', misidentifying legal content, depending on the calibration of the tools.

Importantly, the performance and quality of filtering technologies is by and large dependent on the quality and governance around the database of fingerprints against which filtering is conducted. Considerations on the initial identification and acceptance process for a piece of content to be added to the database are particularly important.

Such technology is highly relevant when video, image or sound files are concerned, but practically unfit for text.

### c. Current use of filters against illegal content and reported accuracy

In the 2015-2016 public consultation several intermediaries pointed to the use of various filtering technologies164. Recently, a few of the major online platforms reported using machine-learning classifiers to flag terrorist or child sexual abuse content. In the latest open public consultation, some large companies confirmed their use of technologies, whereas micro and small enterprises pointed to difficulties in use and accuracy of tools they had experimented with and highlighted complexities in identifying and misidentifying content.

For terrorist content, two such systems are known to be used by the industry. Initially set up amongst four major online platforms, access to a shared database of fingerprints is currently granted to 13 companies. The E-Glyph tool is also available under certain conditions[165]. No other filtering tools are accessible as part of any known commercial offer – to date – and are not part of general content moderation offerings by third parties. For the current, privately-developed solutions, the assessment and decision as to what content to include in the database is taken by the private company, according to definitions and assessment of content as established in their terms and conditions, and not necessarily against legal definitions.

For Child Sexual Abuse Material, the most renowned software used for hash-based filtering is PhotoDNA[166], developed by Microsoft and made available to qualified organizations for free under certain conditions to help detect and report the distribution of child exploitation images. In Europe, the Internet Watch Foundation makes available to its registered members a database of hashes for filtering CSAM, filtering CSAM content against a database maintained by the IWF.

164 e.g. URL blocking based on black-list of Internet Watch Foundation
165https://www.counterextremism.com/press/counter-extremism-project-unveils-technology-combat-online-extremism
166 https://www.microsoft.com/en-us/photodna (last consulted September 3rd 2017)

## 2 OTHER CONTENT DETECTION TECHNOLOGY

Recently, two of the big online platforms have reported to be using machine-learning classifiers to flag content as possible terrorist or violent extremist material. Companies claim high levels of accuracy167 in flagging content for human review, but no data is available on the parameters under which a piece of content is considered to be terrorist material. Companies reported that they had run and trained the supervised learning models for several months, and deployed them accompanied by human review during the training period.

In the public sector, the UK Home Office has reported168 the development of a tool by ASI Data Science to detect terrorist materials online, put at the disposal of companies. Technology is currently trained on Daesh specific types of content and a further iteration of the tool will focus on AQ (the tool has to be tailored according to the terrorist group and its modus operandi). According to the UK Government, tests have shown that the ASI tool can automatically detect 94% of Daesh propaganda with 99.995% accuracy.

For terrorist content, this the development of such technologies needs to build on a very large basis of terrorist content previously identified as well as an even larger control data of 'grey area' content and lawful content. Changes in patterns in the image / video composition of terrorist materials also require retraining of the tools. Experts flag the need to closely couple the deployment of such technology with an observation of the *modus operandi* of the terrorist organisations under observation and keep a vigilant observation of the signals alterations in the video production169.

For text detection, natural language processing is considered by and large immature for identifying illegal hate speech and is not capable of distinguishing between illegal hate speech and other types of violent speech or satire170. Anecdotal reports point to misidentification and takedown of lawful speech171. In addition, as signalled by Mandola Project's best practice against hate speech online, a series of instances such as 'more or less explicit speeches used to denounce illegal speeches on information websites or even art including movies or theatre storyboards' incur the risk of being unlawfully censored by automatic filtering of allegedly illicit speech172.

Generally, machine learning and artificial intelligence are increasingly bringing promising results and progressing in accuracy of predictions in a wide range of application areas. The Commission has recognised the potential of the technology, as well as the need for further R&D&I in this area, most recently through its Communication on Artificial Intelligence. However, pitfalls of the technology are also widely acknowledged, with notorious examples of mis-classification of images having recurrently made the headlines173. Calls for fairness, accountability and transparency have emerged in the past years, as the deployment of the technology increases. The issue is also captured by policy responses at EU level. The GDPR sets very clear principles and

167 No verifiable accuracy reports or independent checks available to date
168 https://www.gov.uk/government/news/new-technology-revealed-to-help-fight-terrorist-content-online
169 See, for example, https://www.wired.co.uk/article/isis-propaganda-home-office-algorithm-asi
170 A. SCHMIDT, M. WIEGAND, 'A survey of hate speech detection using natural language processing' in Proceedings of the Fifth International Workshop on natural Language Processing for Social Media, Spain, April 2017, http://www.aclweb.org/anthology/W/W17/W17-1101.pdf
171 The most recent report involved the misidentification of an article about the US Declaration of Independence as hate speech, https://www.telegraph.co.uk/news/2018/07/05/facebook-censors-americas-declaration-independence-hate-speech/
172 Mandola Project, *ibid.*, p. 30; see also Council of Europe, *ibid.* – describes contextual checks for decisions on the illegality of hate speech.
173 https://www.wired.co.uk/article/chemical-weapons-in-syria-youtube-algorithm-delete-video

safeguards for data subjects subjected to automated processing of their personal data, including profiling, thus mitigating risks of discrimination and unfair treatment of individuals. The Commission is further analysing the opportunities and pitfalls of automated decision-making, and is working on general ethical principles for Artificial Intelligence.

## 3 COSTS OF THE TECHNOLOGIES

Costs incurred by online platforms for setting up voluntary filtering technologies vary depending on the type of files, type of illegal content monitored, and volumes of content uploaded on the platform. Exact data on costs is not easily obtainable and needs to consider development, deployment as well as maintenance cost; however, some self-declared costs were reported by HSPs in the public consultation launched by the Commission in 2016. For sporadic, non-systematic checks on the content hosted, one respondent estimated spending 5% of all operations costs (for a relatively small flux of content and user, hosting text-only content). Other companies developing software for filtering copyrighted content, maintaining databases fed by right holders, an enacting their decision as to the copyright infringing content, estimate a global development cost as high as 100 million USD (video and sound file, very large volumes of data). Similarly, for sound files only and a somewhat lower volume of data, another platform estimates development costs of 5 million EUR, and 12 full time equivalents in engineering and legal expertise.

### a. Further considerations

In interviews with judges from across the EU conducted in June and July 2017, filtering of content was identified by several judges as likely to be of increasing importance in attempts to keep illegal content off the internet in the future, but also as a source of concern given the potential for over-removal. Given such limitations of automatic decision-making, as well as error rates on false positives, the practical use of such filtering algorithms needs to mitigate risks of infringing fundamental rights such as freedom of expression. The governance, risk assessment, and safeguards put in place around the use of such technology are important.



www.parlament.gv.at