BRIEFING

Initial Appraisal of a European Commission Impact Assessment

European Parliament

Preventing the dissemination of terrorist content online

Impact assessment (SWD(2018) 408, SWD(2018) 409 (summary)) accompanying a Commission proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018) 640)

This briefing provides an initial analysis of the strengths and weaknesses of the European Commission's impact assessment (IA) accompanying the above-mentioned proposal, submitted on 12 September 2018 and referred to the European Parliament's Committee on Civil Liberties, Justice and Home affairs (LIBE).

The Commission has presented the proposal in an effort to address what it has identified as 'a very important public policy and security concern in the EU', namely 'the availability and proliferation of illegal content online' (IA, p. 2).

In its 15 June 2017 resolution on online platforms and the digital single market, the Parliament urged 'online platforms to strengthen measures to tackle illegal and harmful content online', and noted in particular the absence of references to content relating to incitement to terrorism in the Commission proposal for a revised Audiovisual Media Services Directive. In its position of 2 October 2018 on that proposal, the Parliament introduced amendments aimed at offering citizens protection from incitement to terrorism, which were subsequently incorporated in the revised directive, adopted on 14 November 2018. However, since the directive is primarily focused on the audiovisual media, only a limited segment of services offered via online platforms is governed by its provisions.

In the conclusions adopted at its meeting of 22 and 23 June 2017, the European Council affirmed that it expected the industry 'to develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts', adding that 'this should be complemented by the relevant legislative measures at EU level, if necessary'. In the conclusions of its meeting of 28 June 2018, it welcomed 'the intention of the Commission to present a legislative proposal to improve the detection and removal of content that incites hatred and to commit terrorist acts'.

The current proposal complements other initiatives in this area. Amongst these, the 2000 E-Commerce Directive provides the general framework for the removal of illegal content by hosting service providers. The 2017 Terrorism Directive establishes minimum rules with regard to the definition of criminal offences, and includes the distribution of online messages with the intention of inciting a terrorist offence in the list of terrorist offences that EU countries must punish as criminal offences. It also obliges Member States to take measures for the prompt removal of online terrorist content that is hosted in their territory and to endeavour to obtain the removal of such content hosted outside their territory.

Non-legislative initiatives include the Commission communication of 28 September 2017 on tackling illegal content online (hereafter 'the communication'), which lays down a set of guidelines and principles for online platforms to counter illegal content online in cooperation with national authorities, Member States and other relevant stakeholders. This was followed by the Commission recommendation of 1 March 2018 on a set of operational measures that companies and Member States could take to effectively tackle illegal content online, with a specific emphasis on terrorist content (hereafter 'the recommendation').

Author: Hubert Dalli with Antonia Albanese
Ex-Ante Impact Assessment Unit

PE 631.731 – January 2019

Problem definition

The IA identifies two problems:

- '[the services of] hosting service providers are abused for the dissemination of terrorist content online [; this practice is] affecting the business models and users' trust in the digital single market';
- 'terrorist content is [not only] accessible online, [but it] reappears and spreads across service providers [,] posing a security challenge'.

The IA sees these problems as arising from four problem drivers:

- hosting service providers face legal fragmentation and uncertainty when operating in different Member States;
- Member States face obstacles in intervening against online terrorist content due to difficulties in contacting and engaging with hosting service providers and the unavailability of removed content to support investigations;
- measures to detect, remove and prevent the dissemination of terrorist content online are not effectively or evenly implemented by hosting services;
- hosting service providers' policies to detect, assess and remove online terrorist content are not transparent enough to allow users and public authorities to monitor companies' action against such content.

The IA clearly identifies the nature of the problem, as well as demonstrates its consequences and discusses how it can evolve. The scale of the problem is explored to some extent with references to Eurobarometer data and to statistics extracted from the stakeholder consultation (the latter is discussed in greater detail in a separate section below) and other sources. The IA notes, however, limitations with regard to the availability of data, which prevent a clearer identification of the scale of the problem.

Objectives of the initiative

The IA identifies the **general** objective of the proposal to be the establishment 'of 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' (IA, p. 21). The **specific** objectives are listed in the table below.

As recommended in the Commission's better regulation guidelines and in tool 16 of its better regulation 'toolbox', the IA sets **operational** objectives after having identified the preferred option and within the context of the discussion on monitoring and evaluation. Except for the specific objective of facilitating the provision of online services across the digital single market by limiting legal fragmentation, the IA sets one or more operational objectives for the specific objectives and lays down corresponding tentative monitoring indicators and the respective data collection strategy.

Specific objectives	Operational objectives	Monitoring indicators	Data collection strategy
Facilitate the provision of online services across the digital single market by limiting further legal fragmentation			
Improve the ability of relevant authorities to intervene against terrorist content online and to combat crime	Increase capacity of Member State authorities to detect, identify and request 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 the accountability of hosting service providers to Member States	Number of companies reporting	Reporting by hosting service providers to Member States
Increase the effectiveness of measures to detect, identify and remove online terrorist content	Ensure that hosting service providers will, within one hour, remove terrorist content notified via removal orders	Number of removal orders and rate of removals within one hour	Reporting by Member States (on the basis of own data and feedback by hosting service providers)
	Ensure a 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 online terrorist content	Number of companies putting proactive measures in place	Reporting by hosting service providers to Member States
		Rate and speed of terrorist content online removal by hosting service providers' own tools	
		Reliability of detection tools	
	Enhance coordination amongst Member States and Europol	Number of Member States connected to Europol for channelling removal orders and referrals	Data provided by Member States and Europol
Increase the transparency and accountability of hosting services for measures taken to detect, identify and remove online terrorist content	Improve awareness of users and citizens on companies' policies and safeguards against online terrorist content	Number of companies publishing transparency reports	Reporting by hosting service providers to Member States
Introduce safeguards against the risk of erroneous removal of legal content and ensure protection of fundamental rights	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	

The objectives correspond directly to the problems identified and to their drivers and consequences, and appear to be specific, measurable, achievable and relevant. The objectives, however, do not appear to be time-bound as required in the better regulation guidelines and in tool 16 of the 'toolbox'.

Range of options considered

The IA describes a number of options that were discarded at an early stage on grounds of effectiveness, coherence or proportionality. It then proceeds to discuss the intervention logic and the options retained for detailed examination. The IA justifies its choice not to retain any non-regulatory options on

the grounds that action against the spreading of terrorist content online is urgent, and that existing voluntary processes have proven insufficient to deal satisfactorily with this phenomenon. Some evidence in this regard is presented in particular in the problem definition. The approach adopted by the IA in respect of the retained options is to use the concept of building blocks: there is a core set of basic measures to address the specific objectives, with the differences between the options being a matter of different intensities of intervention. The three options alternative to the baseline are presented in the table below, with option 3 (in bold) being the preferred one.

Option 1	Option 2	**Option 3**
Narrow definition of terrorist content as material disseminated with the purpose to directly incite a terrorist act produced by EU-listed terrorist organisations	A more comprehensive definition of terrorist content as material disseminated with the purpose to incite, recruit and train for terrorism, including in particular material produced by EU-listed terrorist organisations	**Same as option 2**
Harmonised system of removal orders. Hosting service providers are required to have measures, procedures and tools in place to enable them to remove content within one hour of the receipt of a removal order.	Same as option 1	**Same as options 1 and 2**
Member States have to designate competent authorities, but are not obliged to establish such entities.	Same as option 1	**Member States are obliged to establish competent authorities with the capacity to detect and notify terrorist content.**
Referrals would not be regulated under this option	Requirement for hosting service providers to have procedures in place to make an assessment on referrals from Europol	**Requirement for hosting service providers to have procedures in place to make an assessment on referrals from Europol and Member States**
Proactive measures: hosting service providers are required to carry out a standardised risk assessment, while the development of a remedial action plan is not mandatory but can be done with the involvement of the authorities.	Proactive measures: hosting service providers are required to present a remedial action plan that should contain appropriate measures to prevent the dissemination of terrorist content through their services. Measures may include, as appropriate, automated means to detect, identify and expeditiously remove known terrorist content and prevent resubmission.	**Proactive measures: hosting service providers are obliged to identify and put in place measures to prevent the dissemination of terrorist content through their services. Measures shall include, as appropriate, i) automated means to detect, identify and expeditiously remove known terrorist content and prevent resubmission; and ii) reliable technical means to detect and prevent the appearance of new terrorist content.**
Points of contact are set up within the hosting service providers for the purpose of receiving legal orders.	Points of contact are set up within the hosting service providers for the purpose of receiving legal orders and Europol referrals.	**Same as option 2.**

No obligation for coordination between Member States	Obligation for Member States to keep each other informed and to coordinate and cooperate with each other; possibilities for Member States' cooperation with Europol	**Wider scope for Member States' obligation to keep each other informed and to coordinate and cooperate with each other; wider scope for Member States' possibilities for cooperation with Europol**
Obligation for hosting service providers to report on suspected criminal offences	Same as option 1	**Hosting service providers are required to report on suspected criminal offences and to retain terrorist content for law enforcement purposes.**
Due diligence requirements to avoid erroneous removal of legal content	Same as option 1	**Same as options 1 and 2**
Complaint procedures and judicial redress for hosting service providers and content providers	Same as option 1	**Same as options 1 and 2**
Transparency reports and reporting requirements for the implementation of respective obligations under the option	Same as option 1	**Same as options 1 and 2**
Member States to establish a regime of sanctions under national law and determine rules on jurisdiction	Same as option 1	**Same as options 1 and 2**
Requirement to establish a legal representative for companies established outside the EU	Same as option 1	**Same as options 1 and 2**

The IA appears to make a good comparative presentation that is focused on the similarities and differences between the options, yet remains on a quite general level of description without much deliberation on the finer details of the options. Among the less clear aspects of the options is the issue of Member States' cooperation with each other and with Europol.

Scope of the impact assessment

The IA assesses the options for their expected economic and social impacts. The IA assesses the economic impact with regard to: the functioning of the internal market and competition; businesses, in particular SMEs (where for the preferred option it is estimated that hosting service providers would have to cover the cost of 2 to 11.5 additional full-time employees) and their competitiveness; technological development and the digital market; the administrative burden and costs for public authorities. From the social point of view, the IA considers the impact on: crime, terrorism and security; the safety of internet users; and governance and good administration.

The IA also analyses the impact of the options on international trade relations and third countries. It states that there are no significant environmental impacts to be assessed in the context of the proposal.

When it comes to impacts on fundamental rights, the IA affirms that each of the options may have, to differing degrees, 'both a beneficial and a negative impact on fundamental rights' (IA, p. 40). The IA argues that the options could have negative effects on the freedom to conduct business, the freedom of expression and information, the right to personal data protection and the right to respect for private and family life, by virtue of the added restrictions they impose. However, they could have a positive

impact on of the right to life as a result of the increased security that they would offer. In light of concerns raised by several categories of stakeholders regarding the risk that the options would interfere with fundamental rights and freedoms excessively and disproportionately, the IA discusses a number of safeguards that would accompany the measures envisaged in the options in order to mitigate the said risk.

Subsidiarity / proportionality

The IA dedicates a lengthy section entitled 'Why should the EU act?', to the legal basis of the proposed initiative and to the issue of subsidiarity.

The IA discusses in some detail the choice of Article 114 (on the approximation of laws for the improvement of the internal market) of the Treaty on the Functioning of the European Union (TFEU), as the legal basis of the proposal, rather than Article 83 TFEU (providing for the establishment of minimum rules concerning the definition of criminal offences and sanctions). The IA concludes that an analysis of the problem shows that what is required is a harmonisation of the conditions for hosting service providers to offer cross-border services, and that therefore Article 114 is the appropriate legal basis.

Within the context of subsidiarity, the IA investigates the necessity and added value of EU action. It notes that, with several Member States having already legislated independently on the matter, '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 provide services in the EU' (IA, p. 20). It argues therefore, that this status quo creates the necessity for action at EU level. Furthermore, it affirms that EU action would reduce compliance costs, increase their predictability and enhance legal certainty, thus ensuring that the actions of hosting service providers are streamlined and scaled up, and thereby helping increase their effectiveness.

With regard to proportionality, the IA states that a number of options were discarded for reasons of proportionality, amongst others. Proportionality is also one of the criteria used for the comparison of the retained options, taking into account the ratio between the effectiveness and efficiency of the policy options in reaching the objectives and their potential negative impacts on fundamental rights.

The deadline for the submission of reasoned opinions by national parliaments on whether the proposal complies with the principle of subsidiarity was 12 December 2018. Before that date, the Czech Chamber of Deputies issued a reasoned opinion arguing that the cross-border nature of removal orders seriously infringes the principle of subsidiarity, warning as well about the costs of some of the measures envisaged in the proposal, which it considers disproportionate.

Budgetary or public finance implications

The costs to be borne by EU and national-level public authorities constitute one of the criteria used by the IA in assessing the economic effects of the options. However, the IA observes that in certain instances costs 'are difficult to quantify given that the amount of content is unknown and subsequent follow up actions vary from one Member State to another' (IA, p. 38). The explanatory memorandum accompanying the proposal states that the latter 'does not have an impact on the Union's budget' (explanatory memorandum, p. 9).

SME test / Competitiveness

The IA gives consideration to small and medium-sized enterprises (SMEs), as, according to estimates, more than 90 % of European hosting service providers (around 9 700 companies) are SMEs. The IA notes in particular the SME hosting services' vulnerability to exploitation for the storage and dissemination of terrorist propaganda, and explains that for this reason 'no exemptions are foreseen for SMEs under any of the options' (IA, p. 28). However, it does not appear that the four steps constituting the SME test, according to tool 22 of the Commission's better regulation 'toolbox', have been conducted in this case.

Businesses' competitiveness is one of the impacts that is specifically analysed for each of the options, with the IA discussing in particular how the options affect the use of resources and to what extent they incentivise the development of relevant technologies and mechanisms.

Relations with third countries

All three options target service providers established both within and outside the EU, so long as they offer services within the Union. For this reason, the IA briefly assesses the options' effects on third countries and international relations. The IA concludes that although non-EU companies would have to bear EU regulatory burdens and compliance costs if they offer services within the Union, a knock-on effect of the EU rules – given the global nature of the internet – would result in less illegal content being available online throughout the world.

Simplification and other regulatory implications

The administrative burden inherent in the retained options is another basis on which the IA analyses their likely economic impact. The IA also examines the coherence of the options with the digital single market strategy (in particular the E-Commerce Directive) and with the Terrorism Directive.

Quality of data, research and analysis

The research and analysis undertaken by the IA appear to be predominantly qualitative in nature. Some quantitative analysis was undertaken to calculate the administrative costs that would be incurred by public authorities and hosting service providers; the analytical methods employed for this analysis are described in Annex 4 to the IA. The IA expressly recognises the limitations in terms of data availability, and the assessments and assumptions it makes, given these limitations, appear to be reasonable.

The sources of the data used in the IA vary widely, ranging from studies outsourced by the Commission (which at the time of writing do not seem to be publicly available), to external databases and reports, academic literature, and European and national case law. The calculations of the potential costs for hosting service providers are based on data reported within the context of the various consultation initiatives, as well as data made available by public organisations or in transparency reports.

Stakeholder consultation

The IA reports stakeholders' views throughout the IA; it furthermore identifies those that are affected by the problem or are susceptible to being affected by the proposed options. Annex 2 reports on the Commission's stakeholder consultation strategy, which consisted of three broad phases. The first phase was a fact-finding exercise that allowed 'a clearer definition of the problem space'. A second phase further to the publication of the inception impact assessment 'informed the problem definition and allowed the drawing up of preliminary policy options'. A third phase aimed to inform on the way forward which 'contributed to the design and testing of the policy options' (IA, p. 61). The stakeholder consultation activities feeding into the IA appear to be quite extensive and varied, ranging from bilateral and multilateral meetings with private sector stakeholders and Member States, written submissions in response to the communication and the recommendation, to open public consultations and Eurobarometer surveys.

The open public consultation on measures to further improve the effectiveness of the fight against online illegal content, specific to this initiative, ran from 30 April to 25 June 2018. The IA is vague in justifying the eight-week consultation period – instead of the 12-week period required in the Commission's better regulation guidelines – stating that the shorter period 'was defined in order to ensure that [the] outcome could be used for the preparation of [the] Impact Assessment' (IA, p. 62). It also describes the measures taken by the Commission to mitigate the effect of a shorter consultation by launching the call for contributions on a wide scale. Annex 2 reports that the public consultation received a total of 8 961 replies.

The IA appears to be attentive to the concerns raised by stakeholders, in particular with regard to interference on fundamental rights, and addresses these concerns, amongst others, by including a section describing the safeguards envisaged under the options to mitigate their negative impacts.

Monitoring and evaluation

The IA details the methods envisaged for monitoring and evaluating the initiative. The IA states that the evaluation of the impact of the proposal 'will be based on a detailed programme for monitoring the

outputs, results and impacts', which would set out the indicators and data collection strategy. The IA provides the tentative indicators listed in the table in the section on 'Objectives of the initiative' above, 'subject to further refinement as part of the envisaged monitoring programme' (IA, p. 50).

Commission Regulatory Scrutiny Board

The Commission's Regulatory Scrutiny Board (RSB) issued a positive opinion with reservations on the IA on 25 July 2018, on the understanding that the report would be 'adjusted substantially' to address the 'significant shortcomings' noted by the RSB. The main considerations made by the RSB are regarding the need i) to focus exclusively on terrorist content online in order to reflect the scope and context of the proposal and to explain the urgency of action in this area; ii) to adapt the objectives to reflect the balance between the development of the digital single market, the reduction of terrorist content and the respect of freedom of speech; iii) to adapt the policy options to the scope of the proposal, which is more narrowly linked to terrorist content; and iv) to clarify the safeguard measures, under each policy option, that would ensure proportionality with regard to freedom of expression. The final IA report seems to reflect the RSB recommendations, and in its Annex 1 it describes how these recommendations were addressed.

Coherence between the Commission's legislative proposal and IA

The proposal appears to essentially correspond to the preferred policy option indicated in the IA.

Conclusions

The IA clearly identifies the existing problems and sets objectives that correspond directly to the problems and their drivers and consequences. The IA successfully highlights the differences between the options. However, a fuller description of the individual options would have given a better understanding of how they would function in practice. The analysis of impacts is quite wide-ranging, albeit limited in particular by limited data availability. The IA is particularly sensitive to concerns about encroachment on fundamental rights and freedoms, and makes a distinctive effort to highlight the proportionality of the options and the safeguards they offer for fundamental rights and freedoms.

This briefing, prepared for the Committee on Civil Liberties, Justice and Home Affairs (LIBE), analyses whether the principal criteria laid down in the Commission's own Better Regulation Guidelines, as well as additional factors identified by the Parliament in its Impact Assessment Handbook, appear to be met by the IA. It does not attempt to deal with the substance of the proposal.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)