Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online

1. Introduction

On 12 September 2018, the European Commission published a Proposal for a Regulation on preventing the dissemination of terrorist content online[1] (hereinafter 'the Proposal').

The aim of the Proposal is to establish uniform rules for hosting service providers (hereinafter 'HSPs'), such as social media platforms, video streaming services, video, image and audio sharing services, but also file sharing and other cloud services that make information available to third parties as well as websites where users can make comments or post reviews, who offer their services within the Union - regardless of their place of establishment - to prevent the dissemination of terrorist content through their services and to ensure, where necessary, its swift removal.

The Proposal establishes a minimum set of duties of care for HSPs and sets out various obligations for Member States, notably to enforce the Proposal. In particular, the Proposal introduces the following measures:

- HSPs would have to take appropriate, reasonable and proportionate actions against the dissemination of terrorist content, in particular to protect users from terrorist content (Article 3);

- HSPs would have to remove or disable access to terrorist content within one hour upon receipt of a removal order issued by a competent authority of a Member State (Article 4);

- HSPs would have to assess, on the basis of referrals sent by Member States' competent authorities or by Union bodies (such as Europol) whether the content identified in the referral is in breach of the HSPs' respective terms and conditions and decide whether or not to remove that content or disable access to it (Article 5);

- HSPs would have to implement proactive measures to protect their services against the dissemination of terrorist content, *inter alia* by using automated tools to assess the stored content (Article 6);

- HSPs would have to preserve the content that has been removed and related data which are necessary for the purposes of subsequent administrative proceedings, judicial review and the prevention, detection, investigation or prosecution of terrorist offences (Article 7);

[1] COM (2018) 640 final, Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps europa eu - Website: www edps europa eu
Tel : 02-283 19 00 - Fax : 02-283 19 50

- HSPs would have to establish a relevant complaint mechanism, by which persons whose content was removed pursuant to a referral or a proactive measure can submit a complaint to the HSP (Article 10);

- HSPs would have to provide information to persons whose content has been removed pursuant to a removal order, a referral or a proactive measure (Article 11);

- Member States would have to designate one or several authorities competent to issue removal orders, detect or identify terrorist content and issue referrals to HSPs, oversee the implementation of proactive measures and enforce the obligations established by the Proposal through penalties (Article 17).

The EDPS understands the need to combat the dissemination of terrorist propaganda online and supports the objectives of the Proposal. Nevertheless, he wishes to suggest a number of areas for possible improvements, in order to strengthen the compliance with the fundamental rights to privacy and data protection.

The EDPS takes notice that the Council reached a general approach on the Proposal on 6 December 2018[2]. He welcomes in particular the introduced clarification to the definitions of terrorist content (cf. Article 2 (5) of the Council's General Approach) and HSPs (cf. Recital 10 of the Council's General Approach) as well as the proposed improvement for better cooperation between the relevant competent authorities and Europol (cf. Article 13 (3) and (4) of the Council's General Approach).

2. General comments

Preliminary remarks

The EDPS takes positive note that the Proposal stresses in several provisions that it will ensure the protection of the fundamental rights at stake and that HSPs should always take into account the fundamental rights of the users and also the importance of these rights.[3] In this respect, the EDPS welcomes that Recital 7 of the Proposal explicitly stresses that the Regulation will ensure the rights to respect for private life and to the protection of personal data. In order to strengthen this commitment, he suggests adding an **explicit reference to the applicable data protection legislation**, i.e. the General Data Protection Regulation (EU) 2016/679 (the GDPR)[4] and the Directive (EU) 2016/680 (the Law Enforcement Directive)[5] in Recital 7.

The term '**terrorist content**' is defined in Article 2(5) of the Proposal and encompasses inciting, advocating or glorying the commission of terrorist offences, thereby causing a

[2] 2018/0331(COD), Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online - general approach
[3] For instance Recital 7 and 17 or Article 3 and 6 of the Proposal
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 5 2016, p 1–88
[5] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4 5 2016, p 89–131

danger that such acts be committed (a), encouraging the contribution to terrorist offences (b) and promoting the activities of a terrorist group (c). The EDPS welcomes that the definition is consistent and closely aligned with Directive (EU) 2017/541 on Combatting Terrorism. As Article 3 of Directive (EU) 2017/541 refers with regard to 'terrorist offences' to 'intentional acts', the EDPS suggests to include the term 'intentional' also in the Proposal's definition. This clarification would help to avoid inconsistencies between the two legal texts. However, the EDPS welcomes that Recital 9 of the Proposal clearly sets out that competent authorities and HSPs should take into account the context in which such content appears and that content, which was disseminated for educational, journalistic or research purposes should be adequately protected. Recital 9 of the Proposal also clarifies that the expression of radical, polemic or controversial views in a public debate on sensitive political questions should not be considered as terrorist content.

The EDPS observes that pursuant to Article 4(2) of the Proposal, HSPs should **remove terrorist content within one hour from receipt of the removal order**. In this regard, the Impact Assessment explains that terrorist content is most harmful in the first hours of its appearance because of the speed at which it is disseminated and therefore multiplied. The EDPS shares this sentiment and stresses that terrorist content should be taken down as fast as possible. However, fast removal requires a good cooperation and also a good interaction between HSPs and the competent authorities. Therefore, the EDPS suggests to explore the application of digital signatures for electronically transmitted removal orders and to establish an official and easily accessible list of the competent authorities of the Member States. Thereby, HSPs could quickly verify the authenticity of a removal order and would have quickly available the contact details of the competent authorities in case of doubt.

Commented [BA1]: To me, this is not related to the *timing*, but a general issue of security and authenticity Could we present it as such?

Commented [redacted]2R1]: I left it in, as this was a specific point that GB made during the meeting

The EDPS takes positive notice that pursuant to Article 10 of the Proposal, HSPs would have to establish effective and accessible mechanism allowing content providers, whose content were removed or access to it was disabled, to appeal against the decision of the HSP. In accordance with Article 10(2) of the Proposal, the responsible HSP shall promptly examine the complaint and inform the content provider about the outcome of the examination. The EDPS welcomes the introduction of a **complaint mechanism** as it constitutes an important safeguard against erroneous removals. However, the EDPS considers that the responsibility for the protection and the necessary balancing of relevant fundamental rights belongs ultimately to Member States through their courts or other public authorities He would therefore welcome if a specific provision could be added, to identify the (independent) public authority responsible for reviewing the final decision of a responsible HSP. Procedures should also be envisaged for cases in which the responsible HSP does not react to the complaint of a content provider.

Obligations for HSPs

The EDPS observes that Article 3 of the Proposal would oblige HSPs to take "*appropriate, reasonable and proportionate actions*" against the dissemination of terrorist content, whereas they should "*act in a diligent, proportionate and non-discriminatory manner*" and take "*due regard to the fundamental rights of their users*". While Article 3(2) of the Proposal sets out that HSPs should include in their terms and conditions provisions to prevent the dissemination of terrorist content, Article 6 of the Proposal elaborates that HSPs should also implement proactive measures to protect their services against the dissemination of terrorist content. Along the lines of Recital 18 of the Proposal, such **proactive measures** could consist of measures to prevent the re-upload of terrorist content which has previously been removed,

checking the content against publicly or privately held tools containing known terrorist content as well as using reliable technical tools to identify new terrorist content.

While the implementation of these obligations would be overseen by competent authorities in the Member States, the EDPS observes that the Proposal leaves it widely to the discretion and the responsibility of HSPs to design, establish and implement effective and proportionate measures to prevent the dissemination of terrorist content on their services. In this regard, the EDPS emphasises that it is first and foremost the responsibility of the legislator - and not that of private parties - to ensure that fundamental rights are protected and also that a fair balance between various fundamental rights is struck. Therefore, the EDPS calls upon the legislator to clearly describe in the Proposal the actions to prevent the dissemination of terrorist content or at least to provide further guidance in the Proposals' recitals on how a fair balance between the various fundamental rights can be struck. In any event, the Proposal should avoid a situation in which the protection of fundamental rights is left to the discretion of private entities.

The EDPS observes that Recital 16 and 18 of the Proposal specifically provide that proactive measures may include the use of **automated tools**. The EDPS is aware that due to the vast volume of data, the use of automated tools could be necessary to enable HSPs to successfully search for terrorist content. Nevertheless, the EDPS stresses that the use of such automated tools could require a systematic analysis of all content and also the identification of users which have disseminated terrorist content[6], which in turn would imply processing of their personal data. In this respect, the EDPS draws attention to the fact that compliance with the GDPR will be essential at the implementation stage (e.g. Article 25 of the GDPR). Moreover, and to the extent the use of such tools would amount to profiling or automated decision making in the meaning of Article 22 GDPR, the EDPS stresses the need to comply with the foreseen safeguards, i.e. to provide a **meaningful explanation** of the functioning of the implemented tools (cf. Article 13(2)(f) GDPR), to provide **human verification** for the results of automated tools (cf. Article 22(3) GDPR) and to provide data subjects with the possibility to express his or her point of view and contest the relevant decision (cf. Article 22(3) GDPR).

On the derogation of Article 15(1) of Directive 2000/31/EC

The EDPS observes that pursuant to Article 17(1)(c) of the Proposal each Member State has to designate a competent authority to oversee the implementation of proactive measures by HSPs. In case a competent authority considers that the measures in place are insufficient and no agreement with the relevant HSP can been reached, Article 6(4) of the Proposal provides that the competent authority can issue a decision imposing specific, additional proactive measures on a HSP.

In this respect, Recital 19 of the Proposal elaborates that such a decision "*should not, in principle, lead to the imposition of a general obligation to monitor, as provided in Article 15(1) of Directive 2000/31/EC.*"[7] However, Recital 19 stresses that "*the decisions adopted by*

[6] Cf Article 7, 10 and 11 of the Proposal

[7] See also Recital 23 of the 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: "*The removal of online content constituting a public provocation to commit a terrorist offence or, where it is not feasible, the blocking of access to such content, in accordance with this Directive, should be without prejudice to the rules laid down in Directive 2000/31/EC of the European Parliament and of the Council. In particular, no general obligation should be imposed on service providers to monitor the information which they transmit or store, nor to actively seek out facts or circumstances indicating illegal activity*"

the competent authorities on the basis of this Regulation could ***derogate from the approach established in Article 15(1) of Directive 2000/31/EC****, as regards certain specific, targeted measures, the adoption of which is necessary for overriding public security reasons*" (emphasis added).

The EDPS understands that Recital 19 seeks to constitute a derogation from Article 15(1) of Directive 2000/31/EC and would thereby enable competent authorities to impose a general monitoring obligation on HSPs. The EDPS has serious doubts as to whether a derogation to a directive can effectively be introduced via a preamble to another instrument. At the very least, a possibility to derogate from what has constituted one of the basic principles that has underpinned the development of the internet in the EU since its early days should not be introduced without a proper debate, involving all stakeholders concerned, and carefully weighing all advantages and possible risks. It is also worth recalling that any interference with the fundamental right to data protection must comply with the criteria set out in Article 52(1) of the Charter, including the requirement of having a clear basis in law of sufficient quality.

Moreover, the EDPS stresses that subject to the principle of proportionality, limitations to fundamental rights may be made only if they are necessary. The EDPS considers that the imposition of a general monitoring obligation on HSPs, which would affect a large and undefined number of individuals, irrespective of whether they are under suspicion to disseminate terrorist content or not, would constitute a disproportionate measure exceeding the limits posed by the principles of necessity and proportionality.[8]

In light of the above, the EDPS has strong reservations about the envisaged derogation from Article 15(1) of Directive 2000/31/EC and recommends to reassess the need for such a far-reaching measure.

Preservation of content and related data

The EDPS observes that pursuant to Article 7 of the Proposal, HSPs would be required to preserve removed content and 'related data' for the purpose of subsequent administrative proceedings and judicial review (as a safeguard in cases of erroneous removal) and for the purpose of prevention, detection, investigation or prosecution of terrorist offences ('double purpose')[9].

While the EDPS takes notice that Article 7 of the Proposal does not clearly define the term '**related data**', he observes that Recital 20 of the Proposal only broadly explains that such data "*can include 'subscriber data', including in particular data pertaining to the identity of the content provider as well as 'access data', including for instance data about the date and time of use by the content provider, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the content provider*". The EDPS considers that a clear definition of 'related data' could help HSPs to avoid uncertainties and also help them to comply with their imposed preservation obligation. For these reasons,

[8] See Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others*, para 104-107
On general monitoring in the context of IPR infringements (general monitoring mandates for platforms conflicting not only with Article 15 of the eCommerce Directive, but also with fundamental rights of internet users, including the right to the protection of personal data), see Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs* (SABAM), para 53

[9] See Recital 21 of the Proposal

he suggests to bring more clarification to the term ‘related data’, which could be done, for instance, by providing an exhaustive list of data categories that HSPs should preserve[10].

Brussels, January 2019

[10] As long as HSPs obligations are unclear, there is a risk that HSPs would be ‘incentivized’ by the threat of penalties laid down in the Regulation (cf Article 18(1)(e) referring to Article 7) to collect an excessive amount of data, which will be obviously detrimental to the protection of personal data (as well as to other fundamental rights such as freedom of expression)