From: BUCHTA Anna
To: [redacted]
Cc: [redacted]
Subject: RE: Opinion on terrorist content online
Date: 31 October 2018 13:42:44
Attachments: [redacted] Opinion Online Terrorism+Abu.docx

Dear [redacted]),
Many thanks for this excellent draft. It reads very well and I think we are almost there :) I did, however, insert some suggestions and questions to invite you to possibly fine-tune some points – everything obviously open for discussion, if there is anything I misunderstood or missed!
One thing that I think does not come out very clearly is the issue of public authorities "outsourcing" their functions and imposing responsibility on private parties. Moreover, those private parties will be obliged by law to take measures which by definition will have (negative) impacts on many fundamental rights, but at the same time ***they*** are obliged (by the same law) to ***respect*** those fundamental rights! In a way, I fear that some of our suggestions might make it even "worse", by imposing on those providers obligations that they ***cannot*** fulfil, almost by design. While the actual responsibility to ensure fundamental rights are respected – and an appropriate balance between possibly conflicting rights is struck – belongs to the legislator, as clearly set out by the CJUE in Promusicae. Do you think we could write more about this point?
In terms of presentation, the executive summary reads well, but some messages could perhaps be strengthened/made more visible. What I noted down after reading as possible "main messages" include:
- concerns about introducing a derogation from Art 15 of eCommerce directive – very serious issue and I don't think they are even doing it properly in legal technique sense. (I also think that the issue might be broader than just measures imposed by a competent authority ex-recital 19; already any proactive measure might be caught by this general monitoring, especially since they are so vaguely described in this proposal
- the "outsourcing" issue above (if you agree)
- repository for 2nd purpose: disproportionate and probably not even necessary? Including safeguards and conditions from DRI (this part is brilliant, well done!)
- ADM (to the extent we can justify Art 22 GDPR would apply)
- data protection by design
- need for DPIA/possibly prior check by a DPA

These are just my suggestions, could be completed/changed of course.
I also see that the conclusions do not really mirror the executive summary very well, I would suggest to align them more. Please also check that all the issues listed under conclusions are well covered in the body of text (the alignment with e-evidence on definitions etc. was not mentioned, unless I missed it?).
Many thanks again, happy to discuss of course!
Bon (long) week-end,
Anna

From: [redacted]
Sent: 30 October 2018 11:44
To: BUCHTA Anna
Cc: [redacted]
Subject: RE: Opinion on terrorist content online
So, [redacted]
Thank you again!

I tried to take on board and address all your comments and as much as I could.
Dear Anna,
Please for your review.
Dear [redacted]
All changes are in TCs compared to your last version, I just expanded a bit some footnotes and 'nuanced' the retention for the purpose of double checking by uploaders.
I hope it's fine, does not alter the work.
Thanks a lot.
I remain at your disposal,
[redacted]

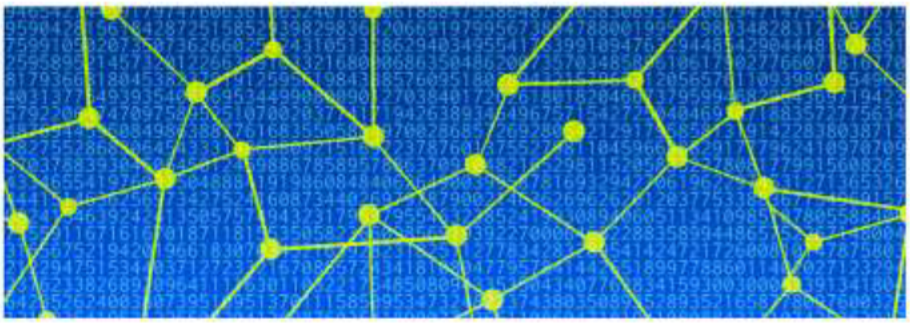
From: [redacted]
Sent: 30 October 2018 09:56
To: [redacted] BUCHTA Anna <anna.buchta@edps.europa.eu>
Subject: RE: Opinion on terrorist content online

And an update to yesterday's rushed version. Also, two more topics that might be considered to add to the opinion (or maybe I overlooked them):
1: An exemption for small hosts, non-commercial hosts, individuals. Not sure if this is already covered by the undefined term "internet society service provider" referred to in article 1.
2: As discussed, the term "third party" is used, while the commissioners in our discussion indicated they meant to cover only *publicly* visible content. Seems a grave mismatch to me.
Regards,
[redacted]

From: [redacted]
Sent: 29 October 2018 20:04
To: [redacted]
BUCHTA Anna <anna.buchta@edps.europa.eu>
Subject: RE: Opinion on terrorist content online

Hi, hereby some comments&suggestions on the draft opinion already; I realised I will be at a conference tomorrow morning until an unknown time, hence I pass you this version in case I do not return before you want to pick up from here (and somehow I still do not have write access to the file on the CMS).
[redacted]

From: [redacted]
Sent: 29 October 2018 17:31
To: [redacted]
[redacted]
Subject: FW: Opinion on terrorist content online



EUROPEAN DATA PROTECTION SUPERVISOR

EDPS Opinion X/2018

on the Proposal for a Regulation preventing the dissemination of terrorist content online

EDPS

xx October 2018

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking - in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. While the EDPS supports the objective~~s~~ ~~to~~ of combat~~ting~~ the dissemination of terrorist content online, thus contributing to a more secure Union overall, he considers that the Proposal should be improved in certain key aspects to ensure compliance with data protection principles.

Executive Summary

This Opinion outlines the position 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.

The EDPS has carefully assessed the Proposal and issues several recommendations to assist the legislator to ensure that the proposed Regulation will be compliant with ~~Union~~ privacy and data protection ~~law~~principles, in particular Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

The EDPS recognises the need to combat the dissemination of terrorist propaganda online, in particular with regard to the potential of such material to groom and recruit new terrorists and to prepare and facilitate terrorist attacks. However, the EDPS underlines that the Proposal in its current form ~~will~~ would have a significant impact on fundamental rights, including the right to freedom of expression and information, the right to an effective (administrative or judicial) remedy, the right to respect of private and family life and the right to the protection of personal data.

While the EDPS welcomes that the Proposal underlines the necessity to take into account the fundamental rights to privacy and data protection, he has serious concerns on aspects of the Proposal that need further evaluation, adjustment and even reconsideration by the legislator, in particular:

- ~~as the proposed measures will have a serious impact on the fundamental rights to privacy and the right to data protection~~ a detailed impact assessment should be conducted;

- ~~the~~ safeguards ~~for~~regarding proactive measures, in particular with regard to the use of automated tools, should be strengthened;

- the proposed obligation for hosting service providers to preserve terrorist content as well as (unspecified) "related data" for the double purpose of administrative or judicial review and for prevention, detection, investigation or prosecution of terrorist offences should be reconsidered;

- the possibility for competent authorities to impose a general monitoring obligation on hosting service providers, which would affect a large and undefined number of individuals, appears to exceed the limits posed by the principles of necessity and proportionality and should be reconsidered.

The Opinion provides further recommendations in terms of data protection and privacy that should be taken into consideration in the legislative process.

Finally, as the Proposal shares relevant similarities with the Proposal on e-evidence, in particular regarding context and terminology, the EDPS calls upon the legislator to ensure a consistent and coherent approach for these two Proposals.

Commented [BA1]: this is a bit repetitive, taking into account the two preceding paragraphs

Commented [2]: Safeguards are *for* users, *against* measures

Commented [3R2]: yes

TABLE OF CONTENTS

Commented [[redacted]4]: page numbering to be re-checked after approval

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to ~~Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and to~~ 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)[2],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[3], and in particular Articles 28(2), 41(2) and 46(d) thereof,

Having regard to ~~Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[4], and to~~ 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 (Law Enforcement Directive)[5],

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

1.1 Context of the Proposal

1. 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").

2. 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.

[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

3. The Proposal builds on HSPs' obligation pursuant to Directive 2000/31/EC[2] to remove illegal content that they store and can be seen as part of a series of regulatory and non-regulatory initiatives to combat illegal content online[3] and also as part of the anti-terrorism package[4].

4. In this regard, the EDPS takes notice that Member States are already obliged by Article 21 of Directive (EU) 2017/541 to ensure the prompt removal of online content that constitutes public provocation to commit terrorist offences and that the revised Audiovisual Media Services Directive[5] will also require Member States to ensure that video-sharing platforms take appropriate measures to protect the public from public provocations to commit a terrorist offence.

5. Moreover, the EDPS observes that the Proposal shares relevant similarities with the Proposal on e-evidence[6] and therefore calls upon the legislator to ensure a consistent and coherent approach[7]. In particular, the EDPS - taking into account his Opinion 09/2018 on Proposals to establish European Production and Preservation Orders to gather e-evidence in criminal matters - recommends to have uniform and clear definitions (Point 4.2), to introduce strong security safeguards for transmissions, including authenticity certificates for removal orders and referrals (Point 5.2.3) and to clarify that legal representatives are not representatives in the meaning of GDPR and the Law Enforcement~~Police~~ Directive (Point 5.2.4).

1.2 Content of the Proposal

6. ~~In t~~The Explanatory Memorandum ~~it is~~ stresse~~d~~s that terrorists misuse the internet for the purposes of grooming and recruiting supporters, preparing and facilitating terrorist activity, glorifying their atrocities and urging others to follow suit.[8] Even though Member States and HSPs have established voluntary partnerships and frameworks to reduce the access~~ibility~~ to terrorist content, it is argued that these measures are not sufficient to

[2] 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'), OJ L 178, 17 7 2000, p 1–16

[3] These initiatives include inter alia Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17 12 2011, p 1–14; 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; COM (2016) 593 final, Proposal for Directive of the European Parliament and of the Council on copyright in the Digital Single Market and most recent COM (2018) 1177 final, Commission Recommendation of 1 3 2018 on measures to effectively tackle illegal content online

[4] 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

[5] COM(2016) 287 final Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities

[6] COM(2018) 225 final, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters

[7] The EDPS observes in particular that Recital 32 of the Proposal already refers to the e-evidence Proposal

[8] In the Impact Assessment it is stated that the terrorist group Daesh produced in the years 2015-2017 an average of 1200 new propaganda items every month (cf Impact Assessment, p 7)

adequately address this issue.[9] However, as Directive (EU) 2017/541 was only to be transposed by Member States by 8 September 2018, ~~the EPDS finds~~ this assumption appears premature.

7. 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 ~~will~~ 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 ~~will~~ would have to assess, on the basis of referrals sent by Member States' competent authorities ~~and~~ 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 ~~will~~ 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 ~~will~~ 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);

   - HSPs will 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);

   - Member States will 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).

8. The EDPS recognises the objectives of the Proposal and also understands the need to combat the dissemination of terrorist propaganda online. However, he wants to stress that the Proposal ~~will~~ as presented by the Commission is likely to have a serious impact on several fundamental rights, including the right to freedom of expression and information, the right to respect of private and family life, the right to an effective remedy, and in particular the right to the protection of personal data.

9. In this regard, the EDPS observes that the accompanying Impact Assessment[10] does not adequately assess the impact of the proposed measures on the fundamental rights to privacy

Formatted: Font: Italic

[9] Explanatory Memorandum, p 1

[10] SWD(2018) 408 final, 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

and data protection[11], nor does it assess the effectiveness of already existing tools. The EDPS emphasises that an impact assessment is not only an important ~~condition~~ element of the Commissions' policy of better regulation[12] but also an essential prerequisite when fundamental rights are at stake[13].

10. The EDPS notes that he was neither consulted by the Commission during the inter-service consultation stage, nor immediately after the adoption of the Proposal. However, due to the serious impact of the Proposal on the rights to privacy and the protection of personal data, the EDPS has decided to issue this Opinion.

2. COMMENTS AND RECOMMENDATIONS

2.1 Preliminary remarks

11. The EDPS observes that the Proposal is based on Article 114 TFEU which provides for the establishment of measures to ensure the functioning of the Internal Market. As the objective of the Proposal is clearly linked to the prevention, detection and investigation of criminal offences, in particular the prevention and combatting of terrorism, the Proposal seems to fall into the scope of Title V of the TFEU. Consequently, ~~T~~the EDPS recommends to re-assess whether Article 114 TFEU is the appropriate legal basis for the Proposal.

12. The EDPS takes ~~notice~~ 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.[14] In this respect, the EDPS observes 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.

13. However, the EDPS notes that the Proposal contains no reference to the applicable data protection legislation, i.e. the General Data Protection Regulation (EU) 2016/679[15] (hereinafter "the GDPR") and the Directive (EU) 2016/680[16] ~~(hereinafter "the Police Directive")~~. Therefore, and for the sake of clarity and legal certainty, the EDPS recommends to insert in the Proposal a specific ~~reference to~~ provision confirming the applicability of the aforementioned legal acts.

[11] The Impact Assessment merely states that the Proposal will interfere with the right to the protection of personal data, and hence any future instrument should have sufficient guarantees to effectively protect personal data (Cf Impact Assessment p 43)

[12] Communication from the Commission to The European Parliament, the Council, The European Economic and Social Committee and The Committee of the Regions Better regulation for better results - An EU agenda and Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making

[13] EDPS, Opinion 9/2017 on the Proposal for a Regulation on the eu-LISA

[14] For instance Recital 7 and 17 or Article 3 and 6 of the Proposal

[15] 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

[16] 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

14. In this regard, the EDPS notes that pursuant to Article 17 of the Proposal, Member States can designate one or more competent authorities with the different tasks laid down in the Regulation. Nevertheless, while the Proposal sometimes specifies the relevant competent authority (e.g. Article 16(4) of the Proposal states "*[...]the competent authority referred to in Article 17(1)(d)[...]*") the EDPS observes that the Proposal lacks this clarity in other instances (e.g. Article 13 of the Proposal merely states "*Competent authorities in Member States[...]*"). As different data protection rules (the GDPR or the Law Enforcement Directive) will apply to the processing of data under the Proposal and subsequently also to the different competent authorities, the EDPS recommends to clarify throughout the Proposal to which specific (category of) authority ~~a~~ every provision ~~does~~ refers to.

15. Furthermore, the EDPS observes that Article 3 of the Proposal provides that HSPs, when taking actions against the dissemination of terrorist content, should take into account "*the fundamental importance of the freedom of expression and information in an open and democratic society*". Nevertheless, as these actions will also have a significant impact on the fundamental rights to privacy and to the protection of personal data, the EDPS recommends to insert in Article 3 of the Proposal a reference to these fundamental rights.

16. 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.[17] However, the Impact Assessment does not provide any evidence that such a short time period is indeed feasible. On the contrary, HSPs highlighted that such a short time limit is deemed unworkable for smaller companies.[18] The EDPS is sceptical whether such a short time period is indeed technically feasible and recommends to reconsider this ~~make it a preferred~~ time-limit on the basis of further analysis to be performed in this regard[19]. ~~rather than a compulsory one~~.

Commented [BA5]: should we not also observe that this appears to shift the burden on operators and possibly put them in a "square the circle" situation where they are supposed to consider fundamental rights while they are *obliged by this legislation* to take measures that *by design* interfere with fundamental rights? In other words, it is first and foremost the responsibility of the legislator to ensure that fundamental rights are adequately preserved in this context, not (only) of the service provider!

Commented [BA6]: appears?

Commented [[redacted]7]: Is "preferred" a sufficiently clear term? Might it be helpful to suggest more concrete wording, e g "where technically feasible"?

Commented [[redacted]8R7]: changed

2.2 On proactive measures

17. Pursuant to Article 6 of the Proposal, HSPs should take proactive measures to protect their services against the dissemination of terrorist content. Recital 18 of the Proposal elaborates that such 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.

18. The EDPS takes notice that pursuant to Article 6 of the Proposal, such proactive measures should be "*effective and proportionate, taking into account the risk and level of exposure to terrorist content, the fundamental rights of the users, and the fundamental importance of the freedom of expression and information in an open and democratic society*". While the EDPS welcomes the commitment to protecting fundamental rights apparent in this

[17] Cf Impact Assessment, p 8
[18] ~~In the Impact Assessment it is stated~~ Cf Impact Assessment, p 86
[19] Such assessment is important also in the light of Article 18(4) of the Regulation, establishing that a systematic failure to comply with removal orders "is subject to financial penalties of up to 4% of the hosting service provider's global turnover of the last business year "

provision, he considers that with regard to the fundamental rights a stronger wording is needed and recommends to replace "*taking into account*" with *"respect*"[20].

19. Furthermore, as Article 6 of the Proposal also refers to the "*risk and level of exposure of the HSP to terrorist content*", the EDPS recommends to introduce in the Proposal an obligation for HSPs, *before* they put in place any proactive measure, to: (i) perform a risk assessment on the level of exposure to terrorism content; ~~and~~ (ii) to draw up a remedial action plan to tackle terrorist content proportionate to the level of risk identified[21]. Thereby, the proactive measures of HSPs would achieve a better targeting and HSPs would also have a useful accountability tool at their disposal.

2.3 On the use of automated tools in the context of proactive measures

20. The EDPS ~~observes~~ notes 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 may be necessary to enable HSPs to search for terrorist content. However, he insists that such automated tools should only be used in a cautious and targeted way, whereas the relevant search parameters should not be based solely on sensitive information, for instance religious beliefs.

21. In this respect, the EDPS ~~wants to~~ recalls that the GDPR introduced in Article 25 the concept of data protection by design and by default. This concept requires controllers to implement appropriate technical and organisational measures in order to effectively ensure compliance with the data protection principles and to integrate the necessary safeguards to meet the requirements of the GDPR and in particular to protect the rights of data subjects. Moreover, the concept requires controllers to ensure that by default only those personal data are processed, which are necessary for the specific purpose of the processing. Therefore, the EDPS recommends to introduce in the Proposal a specific reference to Article 25 GDPR and the concept of ~~privacy~~ data protection by design and by default.

22. Furthermore, the EDPS recalls that Article 22(1) GDPR provides a general prohibition of solely automated individual decision-making, which produces legal effects or similarly significant effects on data subjects. However, Article 22(2) GDPR foresees exceptions to this general prohibition and sets out specific cases and requirements under which such decision-making is permissible. In particular, Article 22(2)(b) GDPR provides that Union or Member States law can authorise such decision-making when it also lays down "*suitable measures*" to safeguard the data subject's rights and freedoms as well as legitimate interests. In this respect, Recital 71 GDPR stresses that such "*suitable safeguards*" should include in any case specific information to the data subject, the right to obtain human intervention, in order to express his or her point of view and to obtain an explanation of the decision reached after such assessment and to challenge the relevant decision.

23. In this regard, the EDPS observes that Article 8(1) of the Proposal provides that HSPs should set out in their terms and conditions their policy on the prevention of terrorism

[20] This would also be in accordance with the wording of Recital 7 of the Proposal

[21] The Impact Assessment refers to these two safeguards, "risk assessment" and "remedial action plan, as alternative options to Option 3 The EDPS considers that Option 1 and 2 refer to a feature that is different from the *scope*, namely to the implementation of *safeguards* for the measures under Article 6 of the Proposal pursuant to a risk-based approach

Commented [BA9]: Again, are we not suggesting to impose on the HSP an obligation that they *cannot* comply with, because the proactive measures they are *obliged* to take *by definition* interfere with such fundamental rights?

Commented [BA10R9]: In addition, should we not at least ask the question how such proactive measures would relate to the general prohibition of monitoring ex- Art 15 eCommerce directive?

Commented [BA11]: Should we clarify when would they have to take these actions?
Would that be before they host any content? If so, that may be a too heavy duty for small hosts, e g an individual setting up a community wiki

[redacted] today: I now see the introduction to the regulation explicitly says (2 4 Proportionality) that obligations on HSPs only occur after a finalised removal order; seems fair It could still be mentioned here for clarity

Commented [BA12R11]: ok, added timing of actions As for removal orders, since HSPs just have to comply, the risk assessment and the remedial action plan do not really make a difference

Commented [BA13]: Again, question: how is this different from a "general obligation to monitor" that HSP must not be subject to according to the eCommerce directive? This could support our call to use automated tools in a "targeted" way (although I have no idea what that would mean in practice ;))

Commented [BA14]: should we add an introductory sentence that in the context of automated screening/filtering it is inevitable that personal data (of users) will be processed? We probably have included something along these lines in the copyright comments?

Commented [BA15]: Can you clarify here why you think this would be applicable? Anything in the EDPB guidelines on ADM that would suggest content filtering "significantly affects"? or legal effects because possible law enforcement action?

content, "*including, **where appropriate**, a meaningful explanation of the functioning of proactive measures including the use of automated tools*" (emphasis added). Moreover, Article 9(1) of the Proposal provides that HSPs should introduce effective and appropriate safeguards to ensure that decisions, which are based on automated tools, are accurate and well-founded. In particular, Article 9(2) of the Proposal provides that such safeguards should consist of "*human oversight and verifications **where appropriate** and, in any event, where a detailed assessment of the relevant context is required [...]*" (emphasis added).

24. While the EDPS welcomes the ~~adopted~~ proposed safeguards, he is of the opinion that a stronger wording is needed and recommends to replace in Article 8(1) and 9(2) of the Proposal the wording "*where appropriate*" with "*in any case*"[22].

25. The EDPS also notes that, pursuant to Article 6(2) of the Proposal; HSPs should submit reports to the competent authorities allowing the latter to evaluate, among others, the functioning of the automated tools. While the EDPS welcomes this provision, he recommends to specify in the Proposal that HSPs should provide the competent authorities with all necessary information about the automated tools used to allow a thorough analysis by the competent authorities and in particular to ensure that these tools will not produce discriminatory, untargeted, unspecific or unjustified results[23].

26. Furthermore, ~~T~~the EDPS ~~also wants~~ wishes to draw attention to Article 35 GDPR which obliges controllers to carry out a data protection impact assessment where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. In accordance with Article 35(3)(a) GDPR, which provides that an impact assessment is imperative in the context of automated individual decision-making, the EDPS ~~considers~~ recalls that HSPs will necessarily have to carry out such an assessment with regard to the envisaged automated tools.

Commented [16]: Comments from
How would one ever "ensure" that a tool is accurate, if it is impossible to automatically detect unlawful content?
Should we ask for the safeguard to explicitly *prohibit* use of automated detectors that have too many false positives?

I see our conclusions contain a line implying this, great: *"decision based on automated tools should in any case be subject to human oversight and human verification"*

Commented [17]: Added a footnote reinforcing need for human verification, see new comment from

Commented [BA18]: this should include in particular the number of "false positives", complaints etc ?

[22] From a 'technical' viewpoint, on the capabilities and limitations of automated content recognition, see "Mixed messages? The limits of automated media content analysis", November 2017, CDT, at page 21: "any use of automated content analysis tools should be accompanied by human review of the output/conclusions of the tool " available at: https://cdt org/files/2017/11/Mixed-Messages-Paper pdf
Another key point highlighted by this paper is the need to provide clear, consistent, precise definition of the type of content to be identified The paper "New EU Proposal on the Prevention of Terrorist Content Online", Joan Barata, CIS, October 2018, points out, at page 5, that "the Directive [Directive (EU) 2017/541 on combating terrorism] requires member States to criminalize the distribution of messages that cause a danger that a terrorist act may be committed, and which advocate for such actions, whereas the proposed regulation additionally refers to incitement The incitement of terrorist acts is a much broader, vaguer and more general legal notion than the advocacy of their commission The Regulation thus appears to give a wider and more discretionary power to State authorities, and creates the possible risk of limiting the expression of certain extreme, but fully legal, ideas or the publication of journalistic work related to terrorism "
This paper is available at:
https://cyberlaw stanford edu/files/publication/files/2018 10 11 Comment Terrorism pdf

[23] See also the "Declaration on Ethics and Data Protection in Artificial Intelligence", adopted at the 40th International Conference of Data Protection & Privacy Commissioners, 23 October 2018, available at:
https://icdppc org/wp-content/uploads/2018/10/20180922 ICDPPC-40th AI-Declaration ADOPTED p
See in particular, point 3, letter c: "Artificial intelligence systems transparency and intelligibility should be improved, with the objective of effective implementation, in particular by: making organizations' practices more transparent, notably by promoting algorithmic transparency and the auditability of systems, while ensuring meaningfulness of the information provided "

27. However, due to the high risk to the rights and freedoms of natural persons and by analogy with Article 36(5) GDPR, the EDPS calls upon the legislator to explore the possibility to introduce for HSPs a mandatory consultation with, and an obligation to obtain prior authorisation from the competent data protection authority.

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

28. 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.

29. 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.*"[24] However, Recital 19 stresses that "*the decisions adopted by 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).

30. 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 recallsing that any interference with the fundamental right to data protection must comply with the criteria set out in Article 52(1) of the Charter, ~~in particular the principle of necessity and proportionality~~including the requirement of having a clear basis in law of sufficient quality.

Commented [BA19]: please feel free to adapt wording, but I hope the idea is clear?

31. Moreover, 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 constitutes a disproportionate measure exceeding the limits posed by the

[24] 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*"

principles of necessity and proportionality.[25] Furthermore, the EDPS reiterates his concerns regarding the "delegated monitoring" of individuals by commercial companies in the context of activities traditionally falling under the competence of law enforcement authorities as regulated under the national law of the Member States and under Union legislation.[26]

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

2.5. Preservation of content and related data

33. The EDPS observes that pursuant to Article 7 of the Proposal, HSPs ~~are~~ 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) as well as for the purpose of prevention, detection, investigation or prosecution of terrorist offences ("double purpose")[27].

34. While Article 7 contains no definition of the term "related data", Recital 20 of the Proposal elaborates 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 ~~recalls~~ considers that a clear definition of "related data" will avoid uncertainties for HSPs and would also ensure legal certainty. He therefore recommends to clearly define the term "related data" and provide an exhaustive list of data categories that should be preserved by HSPs[28].

35. With regard to the double purpose of the envisaged data preservation, the EDPS ~~considers that the retention of removed content and related data for the purpose of subsequent administrative proceedings and judicial review can be justified by the need to enable content providers with effective measures of redress, including the reinstatement of erroneously removed content. However, the EPDS is deeply~~has concerned~~s~~ in particular

[25] 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

[26] EDPS Opinion of 23 June 2008 on the Proposal for a Decision establishing a multiannual Community programme on protecting children using the Internet and other communication technologies; EDPS Opinion of 22 February 2010 on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA); EDPS Opinion of 10 May 2010 on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA

[27] See~~Cf~~ Recital 21 of the Proposal

[28] As HSPs obligations are unclear, there is a risk they would ~~will~~ be 'incentivized' by the threat of penalties laid down in the Regulation -see 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)

Commented [[redacted]20]: An extra critique: if a services provides short-term storage, the 6 months obligation is not helping the user at all

Commented [[redacted]21R20]: If the short term is shorter than 6 months, HSPs should extend it to 6 months I think this Regulation prevails on terms of service

Commented [BA22]: as the same definitions are used in the e-evidence proposal, should we call for consistency between the two?

Commented [[redacted]23]: After further reflections, I would be less categorical on this point HSP could mask, make inaccessible the content, rather than take it down and store it + LEAs would have temptation of accessing the stored data anyway, also if criminal purpose is not envisaged in the regulation
Up to you I would just omit this "considers justified", be super-prudent

Commented [BA24R23]: ok to be cautious, but so I also introduced "in particular" to leave it a bit more open (we might also have other concerns ;))

about the ~~second purpose of~~ necessity and proportionality of establishing the data repository for the second purpose, i.e. to retain content and related data for the purpose of prevention, detection, investigation or prosecution of terrorist offences.

36. The imposition of such a data retention obligation on HSPs would amount to a situation where private entities are required to retain personal data relating to criminal offences for law enforcement purposes for the period of six months.[29] In this respect the EDPS recalls that pursuant to Article 10 GDPR the processing of personal data relating to criminal offences should be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

37. Against the background of Article 10 GDPR, and as the relevant preservation is not under the control of official authority, the provided safeguards have to be appropriate for the rights and freedoms of data subjects. The EDPS observes that Article 7(3) of the Proposal provides that HSPS should "*ensure that the terrorist content and related data [...] are subject to appropriate technical and organisational safeguards*" and that these "*technical and organisational safeguards shall ensure that the preserved terrorist content and related data is only accessed and processed for the [relevant] purposes [...] and ensure a high level of security of the personal data concerned.*"

38. The EPDS recalls that Article 7 of the later repealed Directive 2006/24[30] provided in this respect that "*the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure*"; and that "*the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only*". However, the CJEU concluded in *Digital Rights Ireland Ltd*, that the provided safeguards are not sufficient to ensure effective protection of the retained data against the risk of abuse, unlawful access and subsequent use of that data.[31]

39. Moreover, the EDPS takes notice that the Proposal does not lay down ~~contain any~~ substantive and procedural conditions relating to the access and the subsequent use of the preserved data by "competent authorities", as it was required by the CJEU in the aforementioned judgment.[32] The mere reference in Recital 23 of the Proposal, according to which the Regulation "*does not affect the procedural guarantees and procedural*

[29] In particular Recital 22 of the Proposal provides: "*To ensure proportionality, the period of preservation should be limited to six months to allow the content providers sufficient time to initiate the review process and to enable law enforcement access to relevant data for the investigation and prosecution of terrorist offences. However, this period may be prolonged for the period that is necessary in case the review proceedings are initiated but not finalised within the six months period upon request by the authority carrying out the review. This duration should be sufficient to allow law enforcement authorities to preserve the necessary evidence in relation to investigations, while ensuring the balance with the fundamental rights concerned"* (Emphasis added)

[30] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13 4 2006, p 54–63, repealed by Judgment of the Court (Grand Chamber), 8 April 2014, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others

[31] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd, para 54 - 55 and 65 - 67

[32] See ~~Cf~~ Digital Rights Ireland Ltd, para 61 - 62

investigation measures related to the access to content and related data preserved for the purposes of the investigation and prosecution of terrorist offences, as regulated under the national law of the member States, and under Union legislation" can by no means considered to be sufficient.

40. Furthermore, the EDPS questions the necessity of the data retention obligation on HSPs for the purpose of prevention, detection, investigation or prosecution of terrorist offences, as Article 13(4) of the Proposal already obliges HSPs to promptly inform the competent law enforcement authorities of any evidence of terrorist offences they become aware of. In addition, Article 13(4) of the Proposal provides that HSPs could also, in case of doubt, transmit such information to Europol for appropriate follow up.

41. For all these reasons, the EDPS strongly recommends to reconsider the proposed data retention obligation on HSPs for terrorist content and related data for the purpose of prevention, detection, investigation or prosecution of terrorist offences as laid down in Article 7(1)(b) of the Proposal.

2.6 On the complaint mechanism

42. The EDPS takes notice that pursuant to Article 10 of the Proposal, HSPs are required 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.

43. The EDPS welcomes the introduced obligation for HSPs to establish a complaint mechanism as this constitutes an adequate safeguard against erroneous removals. Nevertheless, he wants to stress that pursuant to Article 8(3) of the Charter the right to data protection has to be subject to the control by an independent authority. As the Proposal does not indicate the possibility for content providers to seek independent redress, the EDPS recommends - for the sake of clarity - to add in the Proposal a specific reference, stating that the final decision of a responsible HSP has to be subject to review by an independent authority. Furthermore, the EDPS recommends to include in the Proposal a legal remedy for cases in which the responsible HSP does not react to the complaint of a content provider.

3. CONCLUSIONS

44. After carefully analysing the Proposal, the EDPS makes the following recommendations:

- the Commission should conduct or make available a detailed impact assessment to assess the impact of the Proposal on the right to privacy and the right to data protection;
- the Proposal should be consistent with the Proposal on e-evidence, in particular with regard to uniform and clear definitions, strong security safeguards for transmissions and authenticity certificates for decisions;

Commented [[redacted] 25]: [redacted] More than insufficient, it appears to contradict the narrative held throughout the proposal E g the recital just above it, 22, even says *"This duration should be sufficient to allow law enforcement authorities to preserve the necessary evidence"* (law enforcement does not even perform the preservation)

Commented [[redacted] 26R25]: two different points:
recital 22 is about retention
recital 23 about access
I see of course they are linked in practice, but conceptually different
So I would not say that they contradict each other

Commented [[redacted] 27]: [redacted] It may be asking too much, but could we suggest giving the right to complain not merely to the content provider, but also to any third party that wishes to view the content but cannot access it anymore? Thus not protecting only the freedom of speech, but also freedom of information

Commented [[redacted] 28R27]: from legal point of view the counterparty of the take down by the HSP is the uploader

Commented [BA29]: I'm not sure about this - 8(3) is about data protection only, and DPA will be competent whether or not it is explicitly stated in this proposal *for data protection issues* We could ask for an independent oversight/review mechanism, but perhaps from the point of view of public authorities ultimately responsible for protecting fundamental rights and ensuring a fair balance is struck, i e no "outsourcing" of functions that are in their essence almost judicial (?) to private parties?

Commented [BA30]: to be reviewed once text finalised, possibly 3-4 main messages and more technical ones for the rest?

- HSPs should be obliged to perform a risk assessment on their level of exposure to terrorism content and to draw up a remedial action plan to tackle terrorist content proportionate to the level of risk identified (Article 6);

- HSPs should fully respect the fundamental rights of its users, when establishing proactive measures (Article 6);

- HSPs should take into account the concept of privacy by design and by default when creating automated tools and should at least conduct a data protection impact assessment (Article 6);

- HSPs should in any case give data subjects a meaningful explanation of the functioning of their implemented proactive measures including the use of automated tools (Article 6);

- a HSPs' decision based on automated tools should in any case be subject to human oversight and human verification (Article 6)

- HSPs should provide competent authorities with all necessary information on automated tools to allow a thorough analysis of these tools, in particular to ensure that no discriminatory, untargeted, unspecific or unjustified results are produced;

- the proposed derogation from Article 15(1) of Directive 2000/31/EC, which would enable the imposition of a general monitoring obligation on HSPs, should be reconsidered (Article 6);

- with regard to HSPs obligation to preserve terrorist content and related data, the term "related data" needs to be precisely circumscribed (Article 7);

- the obligation for HSPs to preserve terrorist content and related data for the purpose of prevention, detection, investigation or prosecution of terrorist offences should be reconsidered in the light of the requirement set out by the case law of the Court of Justice of the European Union (Article 7);

- the decision of a HSP on the complaint brought by the content provider has to be subject to the control by an independent authority (Article 10);

- a legal remedy has to be introduced for cases where HSPs do not react to the complaint of the content provider (Article 10).

45. The EDPS remains available to provide further advice on the Proposal.

Brussels, xx November 2018

Giovanni BUTTARELLI

Notes

[1] ~~OJ L 281, 23 11 1995, p 31~~
[2] OJ L 119, 4 5 2016, p 1
[3] OJ L 8, 12 1 2001, p 1
[4] ~~OJ L 350, 30 12 2008, p 60~~
[5] OJ L 119, 4 5 2016, p 89