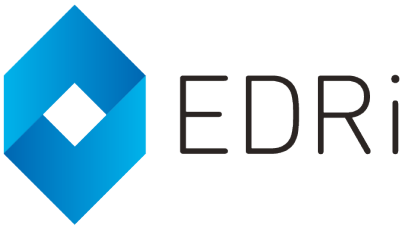

EUROPEAN DIGITAL RIGHTS

Recommendations for the European Parliament's Draft Report on the Regulation on preventing the dissemination of terrorist content online

December 2018

European Digital Rights 12 Rue Belliard, 1040 Brussels https://edri.org twitter @edri tel +32 (0) 2 274 25 70

Introduction/executive summary

European Digital Rights (EDRi) would like to submit the following observations and recommendations regarding the provisions of the proposed Regulation on preventing the dissemination of terrorist content online.

Terrorist attacks are criminal acts that Member States must prevent and react to with targeted, coherent and effective measures.

We stress that the fundamental pillars of European Union law must not be destroyed by terrorism or the threat of terrorism. As a result, **any** measure implemented to fight terrorism must be appropriate, necessary and proportionate. Anything else will be a surrender of the fundamental rights and freedoms in the European Union. EDRi encourages the European Parliament and the Council of the European Union to take the following assessment into account throughout their discussions in the first reading. Together with the undersigned organisations, we call for significant changes to the European Commission's proposal to bring it in line with the Charter of Fundamental Rights and to propose measures that are based on evidence that can achieve its goals.

The undersigned organisations recommend and call for

- evidence based policy making, including the comprehensive assessment of measures set out by the recent Directive on Combatting Terrorism Directive and non-legislative initiatives with regards to terrorist content online;
- application of definitions that are consistent, precise and respectful of human rights, in particular in regard to the definition of a "hosting service provider" and for what constitutes "(illegal) terrorist content;
- consistency of the proposed measures with existing mechanisms and EU primary legislation, requiring in particular:
    - A necessary reform of the measure of referrals, which are issued by competent authorities and significantly threaten the rule of law
    - Removal orders to follow robust and accountable procedures
    - An assurance that proactive measures cannot turn into pre-emptive censorship, and an acknowledgement that the development and use of automated detection tools lacks adequate safeguards for fundamental rights
- Improved transparency and review mechanisms

1. Address the lack of evidence to support the proposal

In the run-up to the publication of the proposal for a Regulation (only 96 hours after the entry into force of the Directive on Combating Terrorism), the Commission conducted several meetings with representatives from industry and Member States. This resulted in a wide range of feedback on possible measures to fight illegal content online and on its respective inception impact assessment[1]. Unfortunately, the concerns and suggestions of civil society, industry and academics were not taken into due account in the proposed Regulation. More problematic, neither the impact assessment nor the legislative proposal itself draws lessons from the wealth of EU experience in fighting illegal content online, including in relation to the wide range of voluntary, self-regulatory measures on either EU or national levels.

In particular, the impact assessment's description of the **scale of the problem** seems to argue against legislative measures. The impact assessment reports that **out of 19 Member States who responded to the Commission's questionnaire on terrorist content online, only two saw an increase in terrorist content online, whereas five did not see any change and 12 reported a decrease**.[2] A Eurobarometer survey found that **only 6% (uncorrected for normal error rates) of the participants had ever come across terrorist material on the internet**.[3] These findings contradict the Commission's assessment that because of this unproven undermining of the Digital Single Market, it is necessary to draft additional legislation in addition to the measures foreseen in the Directive on Combatting Terrorism (which, at the time of writing, has been transposed by only 15 Member States)[4]. It also fails to explain why the non-legislative approach of the EU Internet Forum, whose impact has to this date not been properly addressed and documented either, is inadequate compared to additional legislation.[5]

1 European Commission, *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*, 2018, pp. 85-89, p. 76, available at: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-swd-408_en.pdf (accessed on 31.10.2018)

2 Ibid. p. 83.

3 Ibid., p. 62. It should be noted that approximately 80% of reports of illegal content online are incorrect. On this basis, it is likely that the correct figure is approximately 1.5% (see the excellent statistics page from the Austrian hotline for more information: https://www.stopline.at/en/statistics)

4 Ibid., p. 88.

5 Ibid.

2. Apply consistent, precise and human rights respecting definitions

The proposal continues the tendency of using definitions that are neither in line with other EU legislation regulating the digital single market nor the United Nations guidelines addressing the respect for human rights in the fight against terrorism. The definitions of particular concern are:

- **Definition of hosting service provider:** The definition set out in in the draft Regulation is too broad and covers an extremely large, diverse and unpredictable range of entities. The already imprecise definition is made completely unworkable by the words “in making the information stored available to third parties”. The wording ”third parties” implies that the sharing of stored information could also relate to information shared between a small number of persons (rather than the information being openly accessible), which should not be covered as the shared content is de facto not publicly available.

  In its current form, the definition could cover, for example, a cloud storage service where a user has the theoretical possibility to share his/her access rights with third parties (making the stored content “available” to that third party). It could also cover a restricted online backup of a mailing list, which is only available to its subscribers (“third party” users of the mailing list service and owner of the mailing list). The definition could even cover electronic communications services, such as group chats with a finite number of participants (that may be “third parties”)[6]. In this case, the duty of care and proactive measures would create monitoring obligations for the hosting service provider which directly interfere with the confidentiality of electronic communications and the proposed ePrivacy Regulation.

  Bearing in mind that the stated aim of the text is to prevent the dissemination of illegal terrorist content online, the focus should be on hosting service providers in the traditional sense. Therefore, **only service providers where content is stored for the purpose of making it available to the general public or a group of unknown users, and where electronic communications services are specifically excluded, should be covered.**. Keeping the current definition would widen the range of the types of content and services potentially impacted by removal measures in a way that is unpredictable and unnecessary, which is possibly unintended but nevertheless highly detrimental.

- **Definition of terrorist content:** The UN Special Rapporteur on human rights and counter terrorism[7] made it clear that restrictions to

6 La Quadrature du Net, *Le règlement antiterroriste détruira-t-il Signal, Telegram et ProtonMail?,* 2018, available at: https://www.laquadrature.net/2018/11/26/le-reglement-antiterroriste-detruira-t-il-signal-telegram-et-protonmail/

7 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,* 2016, available at:

fundamental rights, including content removal, should only concern what is, in fact illegal. This Regulation should be limited to *illegal* terrorist content. Consequences of previous failures to take this approach include the work of NGOs reporting on the war in Syria being seriously undermined by blocking of legal content by internet companies[8], which significantly affected the documentation of acts of violence against civilians. These NGOs and the people they are trying to protect are victims of the current balance of incentives of internet companies, which leads to large amounts of utilisable (and thus valuable), legal content being deleted. This balance cannot be further tipped away from freedom of expression – European law should not encourage (or even coerce) hosting service providers to arbitrarily restrict our freedom of expression.

The proposed draft Regulation provides a very broad definition of terrorist content that is similar to – but different from – the definition in the Terrorism Directive (currently being transposed into 27 national EU legal frameworks). The definition includes the following activities:

- inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;
- encouraging the contribution to terrorist offences;
- promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group.

http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session31/Documents/A.HRC.31.65_AUV.docx (accessed on 31.10.2018)

8 Malachy Browne, The New York Times, *YouTube Removes Videos Showing Atrocities in Syria*, 2017, available at: https://www.nytimes.com/2017/08/22/world/middleeast/syria-youtube-videos-isis.html (accessed on 05.11.2018)

While the Terrorism Directive required “intention” to be part of all elements constituting terrorist offences, this draft Regulation omits this necessary requirement. Without considering people’s intentions, we risk that any communication of terrorist-related content, whether for confrontation, reporting, research or historical purposes, will be automatically deleted – with associated personal data being subject to long-term storage. In a democratic society, this is not acceptable. (More on the impact of omitting intention from the definition in Section 3.3.)

EDRi-Recommendation:

The definition of a Hosting Service Provider should relate strictly to entities whose main or primary function is the storage information on behalf of its users in information systems that enable that content to be freely accessed by the public. We suggest the following wording to improve the current text:

“hosting service provider' means a provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored accessible to ***the public****;”*

The definition of what is “(illegal) terrorist content” should be brought further in line with the Directive on Combating Terrorism and needs to be clarified to relate strictly to illegal content. We suggest to use:

“'illegal terrorist content' means one or more of the following information:

(a) inciting ***unlawfully and intentionally the commission of terrorist offences within the meaning of Directive 2017/541 Article 3(1), where such conduct, whether or not expressly advocating the commission of terrorist offences, manifestly causes clear, substantial and imminent danger that one or more such offences will be committed***

(b) ***distributing or otherwise making available by other means online, a message to the public, creating a clear, substantial and imminent danger of****the performance of any of the activities described in Articles 6 to 12 of Directive 2017/541;*

3. Measures proposed in the Regulation must be consistent with existing mechanisms and in line with EU primary legislation

3.1 Necessary reform of the system of referrals by competent authorities that undermine the rule of law

Under the Regulation, competent authorities will have the capacity to notify the hosting service providers about content that *could* be under the scope of the Regulation – even though the authority has never taken, and may never take, action against the content. The hosting service provider would then need to deal with that content under their ostensibly "voluntary" assessment. But if a professional public security agency either can not, or chooses not to, determine whether a certain piece of content is illegal, it seems reckless to devolve regulatory power to a commercial entity.

The approach is evidently based on the competence given to Europol pursuant to Article 4.1.m of the Europol Regulation, which established a voluntary referral system. While we have significant reservations about this approach, the arguments in its favour are worthy of mention.[9] It can be argued that Europol's structure and limited powers justify the non-binding referrals: Europol is a cooperation, rather than an enforcement body, making it impossible for it to issue stronger demands than referrals. Also, as an EU body, it has appeared to be insurmountable for the Agency to assess all 28 Member State laws, which differently transpose instruments on issues such as terrorism and xenophobia. It is of crucial importance to note that in contrast, neither of these two barriers exist for national competent authorities. It is entirely unclear why, on top of the proposed removal orders, the Regulation introduces referrals by (undefined) competent authorities that are not based on law and therefore not in line with Article 52.1 of the Charter of Fundamental Rights of the EU. Therefore, it remains highly questionable whether it is legal, practical or effective to extend the referral system approach to these entities. Instead, it should be considered that when competent authorities in all Member States can issue legally binding removal orders, the arguments justifying a referral mandate for Europol no longer apply. In other words; where legal certainty is created through a system of removal orders, the legal uncertainty created by referrals (regardless of the actor who issues them) can be disposed of.

The Commission has also not been able to clearly answer whether a referral would constitute 'actual knowledge' of the illegality of content that would lead to liability of a company under Art. 14 (1a) of the e-Commerce Directive.[10] Creating legal uncertainty for internet companies as a means of deleting

9 "support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States, the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;"

10 European Parliament, *Answer given by Commissioner Avramopoulos,* 4 April 2018, available at: http://www.europarl.europa.eu/doceo/document/E-8-2017-007205-ASW_EN.html#ref5 (accessed on 31.10.2018)

unwelcome but legal content breaches the freedom to conduct a business, the right to freedom of expression and all the criteria laid down by Article 52.1 of the Charter of Fundamental Rights for acceptable restrictions on fundamental rights[11]. Either the content in question is illegal and dangerous, in which case it should be subject to a removal order, or it is not, in which case involvement of state authorities would clearly not be justified.[12]

In summary, from both a logical and legal perspective, the measure of referrals by national authorities should be removed from the text or restructured in a way which would respect the primary law of the European Union, even though restructuring a fundamentally flawed proposal may not be possible.

EDRi-Recommendation:

Article 5 and all references to referrals in the proposal should be fundamentally reassessed or otherwise deleted. No mechanism that shifts accountability from law enforcement actors to private entities without safeguards and proper assessment of necessity, proportionality, predictability and effectiveness (as **required** by the Charter of Fundamental Rights) should be included in the Regulation.

3.2 Removal orders must follow robust and accountable procedures

The Regulation also proposes removal orders from undefined competent authorities to remove or disable access to illegal content. Where "competent authorities" identify a piece of illegal terrorist content on the internet, there should be a clear, transparent and accountable way to have this content removed, while safeguarding the fundamental rights and freedoms of the individuals. To bring the proposed measures in line with existing law enforcement procedures, a number of changes need to be implemented in the proposal. These relate mainly to the lack of definition of who will be the competent authorities in charge of dealing with removal orders.

The proposal does not give any further indication about what entities can be designated as 'competent authorities'. It is, however, of crucial importance for the principle of due process that such orders are approved by an entity that enjoys clear independence from law enforcement and political authorities.

11 In the US, where Counter Notices are already in place under the Digital Millennium Copyright Act (DMCA), the "number of potentially mistaken or malicious notices still vastly exceeds the number of counter-notices". Daphne Keller and Annemarie Bridy, *DMCA Counter-Notice: Does It Work to Correct Erroneous Takedowns?*, 2017, available at: http://cyberlaw.stanford.edu/blog/2017/01/dmca-counter-notice-does-it-work-correct-erroneous-takedowns#_ftnref6 (accessed on 31.10.2018)

12 Center for Internet and Society, *New EU Proposal on the Prevention of Terrorist Content Online- An Important Mutation of the E-Commerce Intermediaries' Regime*, 2018, p. 8 , available at:, http://cyberlaw.stanford.edu/files/publication/files/2018.10.11.Comment.Terrorism.pdf (accessed on 31.10.2018)

The proposal should therefore make it unequivocally clear that the authorities who will issue the removal orders are independent judicial or administrative authorities. In this way, the assessment of the legality of the content in question will be carried out by an accountable independent entity before a removal order is issued. The European Commission itself stresses heavily that "what is illegal offline is illegal online – any measures that lead to unaccountable removal of content by non-independent authorities would be illegal offline and must therefore not be permitted online.[13]

The authority to issue removal orders and make referrals has extra-territorial effect since any competent authority can issue a removal order or referral to any hosting service provider which is established or represented in the Union. This is a novel feature in EU law, similar to the proposed e-Evidence Regulation. A study on the e-Evidence proposal commissioned by the LIBE Committee has raised several legal issues regarding territoriality.[14] The EU Treaties provide for judicial cooperation between Member States, but the removal orders and referrals in articles 4 and 5 are closer to extensions of competences of national authorities to the territory of other Member States. The legal basis for the proposed regulation is Article 114 of the Treaty on the Functioning of the European Union (TFEU), and not Title V, Chapter 4 of the TFEU, which makes it even more questionable to grant extra-territorial powers to Member States' competent authorities. Several Member States (such as Sweden, Finland and Estonia) have remarked that such jurisdiction may be problematic, and one Member State (Denmark) has even noted that the extra-territorial powers in articles 4 and 5 may be in breach of its Constitution.

The extra-territorial powers to issue removal orders also limit the possibilities and effectiveness of judicial redress for both hosting service providers and content providers, since the removal order must be challenged in the court system of the Member State whose authorities have issued the removal order (recital 8). Last, but not necessarily least, there are ongoing concerns about the rule of law situation in certain Member States. Granting competent authorities in these Member States a wide-ranging authority to order the removal of allegedly terrorist content throughout the European Union could have serious detrimental consequences for freedom of expression and other fundamental rights.

13 European Commission, *Commission Recommendation on measures to effectively tackle illegal content online.* 2018, available at: http://europa.eu/rapid/press-release_MEMO-18-1170_en.html

14 Directorate General for Internal Policies of the Union , Policy Department for Citizens' Rights and Constitutional Affairs, *An assessment of the Commission's proposals on electronic evidence,* pp.34-35, available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf (accessed on 11.12.2018).

EDRi recommendation:

The power to issue removal orders should be restricted to, or at least be authorised by, the competent authority of the Member State where the hosting service provider is established or represented.

3.3 Proactive measures must not turn into pre-emptive censorship

Issues around possible derogation from the E-Commerce Directive and "proactive measures" also need urgent reconsideration.

"Removals under an exception to the E-Commerce Directive Article 15": Although this proposal appears only in a recital, its effect would be enormous. We know from the European Commission's drafting of the proposed Copyright Directive that it does not see an obligation to search for huge numbers of "specific" pieces of information as a "general monitoring obligation". Logically, therefore, it sees possibility for Member States to impose a "general obligation to monitor" that goes beyond searching for specific pieces of known material. Therefore, the proposed derogation to the E-Commerce Directive in recital 15 refers to the automated blanket interception, assessment and removal of content on the basis of algorithmic decision-making. The content would never have been previously identified, would not be subject to a court ruling and would not necessarily be subject to referral to law enforcement authorities.

Proactive Measures refer to a range of different activities to automatically filter content as it is being uploaded. The content being removed could be content that was previously adjudged illegal, content that is part of a database of content removed by a group of cooperating providers but never adjudged illegal, content removed on the basis of a database provided by a third party, or content previously removed by that provider.

The inclusion of pre-emptive deletion (called in the Regulation "proactive measures") formalises the so-called 'voluntary actions' of internet companies, which have been promoted extensively by the European Commission for many years, most recently for instance in the context of the closed-door EU Internet Forum, to unknown effect. Separately, the Regulation proposes a considerable change in the current legal regime set by the e-Commerce Directive and turns these "proactive measures" into an obligation for all relevant service providers offering services to individuals or organisations in the EU. This is a major change on how the internet works and how it will work from now on. As we have argued in the past (namely around debates on upload filters)[15], the change in the liability regime of platforms appears designed to encourage the

15 See for instance Diego Naranjo, *Compulsory Ffltering instead of Obligatory filtering – A compromise?*, available at https://edri.org/copyright-compulsory-filtering-instead-of-obligatory-filtering-a-compromise/ (accessed on 05.11.2018)

use of upload filters as a tool for internet companies to avoid being found liable for illegal content or legal content made available illegally.

Apart from assertions that the content in question is moving to smaller platforms, for which no evidence was provided in the impact assessment, the European Commission has failed to provide any justification for why current practices need to be both extended and made legally binding. The Commission has also failed to provide any evidence that the current practices of members of the Internet Forum are having any meaningful effect. Finally, the Impact Assessment contains no evidence proving that these practices are not being circumvented or that they are not making the situation worse.

EDRi maintains strong reservations against any form of “proactive measures” (namely upload filters), since they are error prone, invasive and, in the Commission’s own assessment,[16] likely to produce ‘false positives’ of judging legal content as illegal, meaning nothing less than a profound danger for the freedom of expression, with little evidence of effectiveness.

The use of automated detection tools to achieve the goals of the proposed Regulation lacks proper transparency, accountability and redress mechanisms.

Therefore, we maintain that any legislation that encourages hosting service providers to treat uploaded content in a prescribed way needs to:

1. Explicitly reject unaccountable automatic removal of content: The Regulation must respect the restriction on general monitoring obligations as recognised in Article 15 of the e-Commerce Directive[17] and related case law of the Court of Justice of the European Union (CJEU)[18]. The proposed Regulation must not derogate from this principle. Any “proactive measures” expected from hosting service providers will mean in practice that these companies will need to implement software capable of automatically recognising content in order to prevent that certain content is accessible online to a general public (or, if the definition of a hosting service provider is not refined, even a closed audience). Such filters are notoriously incapable of distinguishing legal and illegal content, for example by generally failing to take into consideration the context of where the content appears, and are unlikely to improve significantly. There is a need for the assessment of existing rules and any gaps around the development and use of automated detection tools to ensure that both the private and public sector protect and respect fundamental rights and develop adequate mechanisms for transprency, accountability and redress.

2. Eliminate incentives for over-removal of content: The European Commission’s proposal significantly shifts the balance of incentives for service providers – making it preferable to delete more content, more quickly, with no incentives to defend legal content that they host. In the proposed Regulation hosting service providers would maintain their liability protections for content hosted on their servers *as long as* they actively search for and delete content.

16 Commission Impact Assessment, *op cit.*, p. 143.

17 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'), Art. 15.

18 Cases C-275/06 *Telefónica v. Promusicae,* para. 68, 69, C-70/10 *Scarlet Extended*, para. 35, 40, and C-360/10, *SABAM v. Netlog,* para.33-36, 48, 49.

These searches are made easier by the fact that they are protected from any assumption constructive knowledge, implicitly even if this leads to a level of knowledge that the CJEU deemed to amount to "actual knowledge" of illegality. By taking this approach, the European Commission appears to be more driven by the demands of a trade association representing internet giants[19] than by the case law of Europe's highest court[20].

3. Implement effective remedies and safeguards: In order to strengthen the rights of citizens vis-a-vis companies who host and may delete their legal content, the procedures for removals of content should implement strong safeguards with respect to fundamental rights and freedoms. In particular, there should be demonstrably independent, accessible, timely and transparent redress mechanisms. Specific regard should be given to the obligation imposed by the CJEU in the Telekabel case, in which the Court ruled that "[n]ational procedural rules **must** provide a possibility for internet users to assert their rights before the court once the implementing measures taken by the internet service provider are known" (emphasis added).[21]To this extent, it should be made clear that the established complaint mechanism does not constitute the exclusive means of appeal, and that the applicable laws and procedures of Member States continue to apply.

EDRi-Recommendations:

The possibility for a derogation from Article 15 of the eCommerce Directive should be deleted from the text.

References to "proactive" measures should not be maintained in the final Regulation. For all content removals, meaningful human intervention in the removal procedures of hosting service providers should be explicitly included in the text. The proposal should also clarify that redress mechanisms put in place by hosting service providers do not constitute the sole redress mechanism for citizens.

19 The CCIA asked for their liability protections to be protected if their private law enforcement measures "exceed their legal obligations". Computer and Communications Industry Association, *The EU Should Strengthen, Not Weaken, Intermediary Liability Protections*, 2015, available at: https://www.ccianet.org/2015/04/the-eu-should-strengthen-not-weaken-intermediary-liability-protections/ (accessed on 05.11.2018)

20 Case 275/06 *Promusicae v Telefónica*, *op cit.*, Case C-314/12, *Telekabel v. Constantin*, para. 63.

21 Case C-314/12, *Telekabel v. Constantin, op cit,,* para. 57.

4. Improve transparency and review mechanisms

As discussed in Sections 2 and 3, specific safeguards for the freedom of speech and right to information are needed in the Regulation. To ensure sufficient transparency and efficiency monitoring in the pursuit of all restrictions on citizens' fundamental rights, EDRi furthermore recommends that citizens always be presented with adequate information on their rights and redress options. This relates especially to:

Information to be provided by hosting service providers after removal of content or disabling access to it: Information on the outcome of a complaint procedure should contain information on the legal basis of the removal. Hosting services should proactively explain the legal basis for removal of content and details of effective, accessible and timely complaints mechanisms.

Adequate review mechanisms and information on the implementation of the Regulation need to be added in the text: The Commission has been unable to answer a parliamentary question whether the removals following referrals by Europol had inspired any form of follow-up investigation or prosecution of the alleged perpetrators.[22] In order to assess the efficiency, proportionality and appropriateness of the proposed mechanisms, it is not sufficient to simply give the number of removals and the number of complaint procedures launched. In order to evaluate if the legislation is applied adequately and that the measures have led to a significant improvement on the problem of the dissemination of terrorist content, it is absolutely necessary to obtain from hosting service providers and from the competent authorities anonymised data regarding the amount of times the content was accessed before being removed, the total number of items removed on the basis of terms of service, the total amount of items removed on the basis of alleged illegality, the total number of investigations and prosecutions launched in relation to takedown orders, and the proportion of successful prosecutions and statistics on the number of times stored data is accessed by law enforcement authorities.

In order to find and implement appropriate solutions to any problem, it is crucial to assess the issue accurately. This should happen on the basis of benchmarks, against which the proportionality, success or failure of policy initiatives can be assessed. We recommend the development of benchmarks on the basis of criteria listed above.

22 European Parliament, *Answer given by Mr Avramopoulos on behalf of the Commission*, 2017, available at: http://www.europarl.europa.eu/doceo/document/E-8-2017-001772-ASW_EN.html (accessed on 31.10.2018)

EDRi-Recommendation:

Where content is removed, individuals should, as soon as possible after the law enforcement agencies and the judicial authorities do not need to keep the secrecy of the procedure, be informed of the legal basis for the removal. In addition to the annual reports of hosting service providers, law enforcement agencies should produce reports containing the number of requests from different authorities, the number of removals and any other related information derived from the application of the Regulation which could have an impact on fundamental rights of the individuals, specifically regarding their freedom of speech and their right to privacy. In addition to this, statistics should be made available related to the follow up investigations derived from the measures proposed on this Regulation and how many of them have led to significantly reduce terrorist threats both online and offline.

5. Conclusion

The proposed Regulation lacks evidence to achieve its alleged objectives and it would lead to manifest violations of fundamental rights. It increases the risk that legitimate political speech and commentary will be captured and that it will be left for the courts and lengthy procedures to define the substance and boundaries of the scope of the proposed Regulation. This would lead to uncertainty for users, hosting service providers, and law enforcement and the Regulation would fail to meet its alleged objectives.

EDRi urges policy makers not to rush the discussion regarding this Regulation, to significantly improve the text and to seriously take into account the concerns raised in this policy paper in regard to the respect for fundamental rights. In particular, the **definitions of a hosting service provider and terrorist content should be substantially improved** and the **undermining of the rule of law through unaccountable referrals that privatise law enforcement should be prevented.** Likewise, measures in this Regulation should not incentivise companies to pre-emptively and extensively disable access to content or delete content using content recognition technologies. **Companies should also not be incentivised to use automated means of identifying content.** The proposal to permit Member States to derogate from Article 15 of the E-Commerce Directive is entirely unjustified and should therefore be removed.

To safeguard the rights of citizens in the proposal, the **provisions on transparency, competent authorities and redress mechanisms for individuals need substantial improvement**. In particular, **individuals whose content is removed need to be clearly informed as to why this happened**, **and should be directed towards an appropriate, accessible redress mechanism.** Finally, to monitor the efficiency of the Regulation and its impact on fundamental rights, **hosting service providers or law enforcement agencies shall publish reports on a regular basis**, which should include a comprehensive set of benchmarks as described in this paper.

It is up to MEPs and Council Members now to bring a proposal that lacks a proper evidence base and support from key stakeholders in line with the values of the Union.