Council of the European Union
General Secretariat

Interinstitutional files:
2018/0331(COD)

Brussels, 02 September 2019

WK 9235/2019 INIT

LIMITE

ENFOPOL	**TELECOM**
CT	**FREMP**
JAI	**AUDIO**
COTER	**DROIPEN**
CYBER	**CODEC**

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	General Secretariat of the Council
To:	Delegations
N° Cion doc.:	12129/18
Subject:	Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications

Delegations will find attached opinion of the European Union Agency for Fundamental Rights in relation to the above-mentioned subject.

FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

FRA Opinion – 2/2019

[Online terrorist content]

Vienna, 12 February 2019

Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications

Opinion of the European Union Agency for Fundamental Rights

Luxembourg: Publications Office of the European Union, 2019

PDF ISBN 978-92-9474-244-5 doi:10.2811/818523 TK-01-19-164-EN-N

Contents

Acronyms **4**

Opinions **6**

Introduction **13**

1. Enhancing respect for fundamental rights by providing a clear definition of terrorist content and its dissemination **17**

1.1 Enhancing the foreseeability and clarity of the definition of terrorist content 17

FRA Opinion 1 19

1.2 Clearly limiting the scope of the proposal to content disseminated in the public 19

FRA Opinion 2 20

1.3 Excluding certain forms of expression from the scope of the proposal 21

FRA Opinion 3 22

2 Strengthening fundamental rights safeguards on removal orders **23**

2.1 Safeguarding fundamental rights through effective judicial supervision 23

FRA Opinion 4 25

2.2 Avoiding disproportionate impact on the freedom to conduct a business 26

FRA Opinion 5 28

2.3 Ensuring additional safeguards in cross-border removal orders by involving the authorities and courts of the host Member State 28

FRA Opinion 6 29

2.4 Providing sufficient information to content providers as a precondition for exercising the right to an effective remedy 30

FRA Opinion 7 32

2.5 Introducing clear safeguards in relation to preserved content that has been removed or disabled 32

FRA Opinion 8 33

3 Adjusting the referrals' mechanism to avert unlawful interferences with fundamental rights **35**

3.1 Strengthening Member States' obligation to protect fundamental rights online 35

FRA Opinion 9 37

4 Establishing proactive measures that respect the fundamental rights of users and hosting service providers **38**

4.1 Safeguarding due diligence 38

FRA Opinion 10 40

4.2 Ensuring the right to an effective remedy for hosting service providers against decisions imposing additional proactive measures 41

FRA Opinion 11 42

Acronyms

Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union (CJEU is also used for the time predating the entry into force of the Lisbon Treaty in December 2009)
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
ICCPR	International Covenant on Civil and Political Rights
TEU	Treaty on European Union
UN	United Nations

THE EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA),

Bearing in mind the Treaty on European Union (TEU), in particular Article 6 thereof,

Recalling the obligations set out in the Charter of Fundamental Rights of the European Union (the Charter),

In accordance with Council Regulation (EC) No. 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (FRA), in particular Article 2 with the objective of FRA "*to provide the relevant institutions, bodies, offices and agencies of the Community and its EU Member States when implementing Community law with assistance and expertise relating to fundamental rights in order to support them when they take measures or formulate courses of action within their respective spheres of competence to fully respect fundamental rights*",

Having regard to Article 4 (1) (d) of Council Regulation (EC) No. 168/2007, with the task of FRA to "*formulate and publish conclusions and opinions on specific thematic topics, for the Union institutions and the EU Member States when implementing Community law, either on its own initiative or at the request of the European Parliament, the Council or the Commission*",

Having regard to Recital (13) of Council Regulation (EC) No. 168/2007, according to which "*the institutions should be able to request opinions on their legislative proposals or positions taken in the course of legislative procedures as far as their compatibility with fundamental rights are concerned*",

Having regard to the request of the European Parliament of 6 February 2019 to FRA for an opinion "on the key fundamental rights implications of the proposal for a Regulation on preventing the dissemination of terrorist content online (2018/0331 (COD))",

SUBMITS THE FOLLOWING OPINION:

Opinions

1. Enhancing respect for fundamental rights by providing a clear definition of terrorist content and its dissemination

FRA Opinion 1: Enhancing the foreseeability and clarity of the definition of terrorist content

The definition of terrorist content in the proposal draws on definitions of terrorist offences under Directive (EU) 2017/541 (Terrorism Directive), which are however construed for the purposes of criminal proceedings. Furthermore, the proposal deviates from the Directive in important aspects. Article 2 (5) (c) referring to "promoting the activities of a terrorist group"; (d) referring to "instructing on methods or techniques for the purpose of committing terrorist offences"; and, in particular, (b) referring to "encouraging the contribution to terrorist offences". These all potentially broaden the concept of terrorist content beyond that foreseen by the Terrorism Directive. This gives rise to a risk of unlawful interference with fundamental rights, in particular the right to freedom of expression guaranteed in Article 11 of the Charter.

To ensure that it will only apply to content which would manifestly fall under the scope of the Terrorism Directive, the EU legislator should amend proposed Article 2 (5) as follows:

"(5) 'terrorist content' means information which, in a manifest manner:

> ***(a) incites or advocates, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;***
>
> ***(b) promotes the activities of a terrorist group, in particular by inciting, soliciting or advocating persons or a group of persons to participate in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way; or***
>
> ***(c) provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques, for the purpose of committing, or contributing to the commission of, terrorist offences."***

FRA Opinion 2: Clearly limiting the scope of the proposal to content disseminated in the public

Unlike the Terrorism Directive which covers content disseminated to the "public", the proposal applies to any content that becomes "available to third parties". This broad formulation means that the Regulation could be interpreted as applying to private communication – emails, private messaging and cloud infrastructure services – which would represent a disproportionate and unjustified interference with the freedom of expression and information under Article 11 of the Charter and the right to private and family life under Article 7 of the Charter.

The EU legislator should ensure that the proposed Regulation does not apply to expression which does not enter the public domain, disproportionately interfering with the rights to freedom of expression and private life and correspondence of internet users at large. Accordingly, the EU legislator should consider:

- ***replacing in Recital (10) the term "third parties" with "the public";***

- ***replacing in Article 2 (1) and (6) the term "third parties" with "the public";***
- ***adding the term "public" before "dissemination" in Article 1 (1) (a).***

FRA Opinion 3: Excluding certain forms of expression from the scope of the proposal

The preamble of the proposal acknowledges the need to ensure that certain protected forms of expression are respected. Nevertheless, the proposal lacks provisions that would explicitly oblige competent authorities and courts to exclude dissemination of content for legitimate purposes, notably informing the public of matters of public interest and promoting education, academic and scientific research, or literary or artistic expression.

The EU legislator should ensure that forms of expression such as journalistic, academic and artistic expression are adequately protected, such as by considering introducing in Article 1 of the proposal a new paragraph (3), in line with Recital (9), providing that "Content disseminated for educational, journalistic, artistic or research purposes or awareness raising activities against terrorism is excluded."

2. Strengthening fundamental rights safeguards on removal orders

FRA Opinion 4: Safeguarding fundamental rights through effective judicial supervision

Removal orders as regulated in Article 4 of the proposal require hosting service providers to remove or disable access to content identified by the competent authority as terrorist. The proposal does not guarantee any type of involvement of an independent judicial authority in the adoption or prior to the execution of the removal order. At the same time, neither the content provider nor the hosting service provider are afforded a mechanism to effectively challenge the order before the removal is carried out. Combined with the limitations on access to an effective remedy once the removal has already taken place, this offers insufficient protection to the rights at stake, in particular freedom of expression and information and freedom to conduct a business under Articles 11 and 16 of the Charter.

In order to ensure that removal orders are always based on an independent and impartial assessment, the EU legislator should prescribe that the competent authority responsible for issuing removal orders be an independent judicial authority.

Alternatively, the EU legislator could consider:

- ***amending Article 4 (1) by stating that where the competent authority is not a judicial authority, or where the removal order is not based on a judicial authority's decision, the removal order addressed to the hosting service provider shall be at the same time submitted for review to an independent judicial authority determined in accordance with national law; this judicial authority shall notify the competent authority and the hosting service provider of its decision within twenty-four (24) hours from the receipt of the removal order;***

- ***adding in Article 4 (2) that where the judicial authority conducting a review pursuant to paragraph (1) issues a decision that does not confirm the removal order's legality, the competent authority shall ensure the immediate restoration of such content, provided it has already been removed or access to it disabled.***

FRA Opinion 5: Avoiding disproportionate impact on the freedom to conduct a business

The proposed rules for the implementation of removal orders will have considerable implications on the operation of hosting service providers. The time limit of one hour to comply with the removal order, which applies to all host service providers and any content – irrespective of whether it poses an imminent threat – is significantly stricter than the current practice among EU Member States. It may represent a disproportionate restriction to the freedom to conduct a business under Article 16 of the Charter, especially with regard to smaller businesses. It could also lead to automation in the processing of removal orders, with a further negative impact also on the freedom of expression and information of users under Article 11 of the Charter.

In order to avoid disproportionate impact of removal orders on the operation of hosting service providers and the risk of further negative effects on fundamental rights, the EU legislator should consider:

- ***amending Article 4 (2) of the proposal as follows: "Hosting service providers shall remove terrorist content or disable access to it within twenty-four (24) hours from receipt of the removal order. In exceptional circumstances where the competent authority stipulates in the removal order that the particular content poses an imminent threat, hosting service providers shall remove terrorist content or disable access to it within a period shorter than twenty-four (24) hours from receipt of the removal order. The period shall be specifically defined by the competent authority in the removal order; and it cannot be less than one hour from receipt of the removal order, taking into account the time zone, working days and hours of the addressee hosting service provider."***
- ***amending Article 4 (4) of the proposal to provide that the detailed statement of reasons should contain, where applicable, also the reasons which require removing of the content or blocking access to it within less than twenty-four hours.***

FRA Opinion 6: Ensuring additional safeguards in cross-border removal orders by involving the authorities and courts of the host Member State

In cases of cross-border removal orders, the proposal creates a system in which an order issued by one Member State cannot be challenged in the Member State in which the hosting service provider is established (or in which it has a designated legal representative). In line with the basic principles of territorial jurisdiction and related ECtHR case law, the host Member State must be empowered to review the removal order in cases where there are reasonable grounds to believe that fundamental rights are impacted within its own jurisdiction. At the same time, in line with the right to an effective remedy enshrined in Article 19 TEU and Article 47 of the Charter, each natural or legal person has the right to an effective remedy before the competent national tribunal against any of the measures which can adversely affect the rights of that

person. Accordingly, the right should include the possibility for hosting service providers and content providers to effectively contest the removal orders before a court of the host Member State, where it is different from the issuing Member State.

The EU legislator should ensure that cross-border removal orders are regulated in a manner which provides sufficient safeguards to the affected fundamental rights, including by providing access to an effective remedy. The EU legislator should address this explicitly in the relevant substantive provisions by:

- ***requiring the issuing Member State to notify competent authorities in the host Member State, alongside the hosting service provider, of the removal order when it is issued;***
- ***introducing additional safeguards to ensure access to an effective remedy, by providing in substantive articles for the possibility of effectively challenging the removal order before a competent court of the host Member State.***

FRA Opinion 7: Providing sufficient information to content providers as a precondition for exercising the right to an effective remedy

The proposal does not ensure that the content provider receives a copy of the removal order, which represents the legal basis for the removal, contains important information not available through other means, and would be necessary to challenge the measure effectively before the courts. Neither does it ensure that the content provider is informed about the available legal remedies against such orders. Therefore, the proposal does not guarantee that content providers have full knowledge of all relevant facts needed to decide whether and on what grounds they will challenge the removal order. As a result, the proposed Regulation does not provide for minimum safeguards ensuring the effectiveness of a remedial action and legal scrutiny by judicial bodies in line with Article 47 of the Charter.

The EU legislator should ensure that the content provider can receive, at the latest after the removal or disabling of access to the content, a copy of the removal order and information about available legal remedies to effectively exercise its right under Article 47 of the Charter. For this reason, the EU legislator should consider amending:

- ***Recital (26) fifth sentence, to state: "Further information about the reasons for the removal, as well as a copy of the removal order and information of the possibilities for the content provider to contest the decision before a court should be given upon request."***
- ***Article 4 (4), to state: "Upon request by the hosting service provider or by the content provider, the competent authority shall provide a copy of the removal order including a detailed statement of reasons, and any information about the available legal remedies to appeal against removal orders before a court, without prejudice to the obligation of the hosting service provider to comply with the removal order within the deadline set out in paragraph 2."***
- ***Article 11 (2) to add the following: "[…] and shall provide him or her with a copy of the removal order issued according to Article 4 upon request."***

FRA Opinion 8: Introducing clear safeguards in relation to preserved content that has been removed or disabled

Article 7 of the proposal envisages that data preserved following removal orders may later be accessed for investigatory or prosecutorial purposes. Nonetheless, it does not require that such access depend upon prior review by a court or independent administrative body. The proposal also does not clearly stipulate the requirement to erase any data preserved following their preservation period. According to the CJEU and ECtHR jurisprudence, sufficiently clear rules are required to safeguard the rights to personal data protection and private life under Articles 7 and 8 of the Charter.

The EU legislator should accompany the requirement for hosting service providers to preserve content that has been removed or disabled as a result of a removal order with sufficiently specific safeguards. For this reason, the EU legislator should consider:

- ***stating in Recital (23) that "Member States should lay down clear and precise rules indicating in what circumstances and under what conditions competent national authorities can access the preserved content and any related data. Access to such content and data must be subject to a prior review by a court or independent administrative body, except in cases of validly established urgency."***
- ***adding a sentence at the end of Article 7 (1) stating that "Except in cases of validly established urgency, access to terrorist content and related data for any of the purposes under point (b) shall be authorised only after a prior review by a court or other independent administrative authority according to national legislation."***
- ***adding a new second sentence in Article 7 (2) stating that "Related data preserved shall be erased after this period." The same requirement could be reflected in Recital (22).***

3. Adjusting the referrals' mechanism to avert unlawful interferences with fundamental rights

FRA Opinion 9: Strengthening Member States' obligation to protect fundamental rights online

The proposal does not sufficiently justify the necessity of introducing the mechanism of referrals under Article 5 through which competent authorities could instruct hosting service providers to assess specific content against their terms of service and community standards, and potentially remove it. If they are introduced alongside other measures in the proposal, particularly mandatory removal orders, without clearly distinguishing the circumstances in which they should be used, it carries the risk of expanding the scope of what is understood as terrorist content, blurring the responsibility for assessing the online content and undermining the legal certainty regarding liability of hosting service providers. These implications, together with the proposed system of penalties, could lead to a chilling effect on the freedom of expression and information protected under Article 11 of the Charter.

The EU legislator should introduce clear rules to distinguish between content that would justify issuing a removal order, and other terrorist content which would require resorting to a referral.

Furthermore, the EU legislator should consider omitting the reference to Article 5 and referrals in Article 18 (1) (c) requiring Member States to introduce penalties upon hosting service providers.

Finally, the EU legislator should consider including a reference to the positive obligation of the Member States to secure the effective exercise of fundamental rights and prevent fundamental rights violations in a relevant recital.

4. Establishing proactive measures that respect the fundamental rights of users and hosting service providers

FRA Opinion 10: Safeguarding due diligence

By introducing in Article 6 a broad obligation upon hosting service providers to apply proactive measures to assess and potentially remove content and at the same time making them fully responsible for potential interferences with fundamental rights, the proposal raises issues of compatibility with the positive obligations of the state under the Charter. Obligations under the proposed Article 6 may lead to general monitoring of content, which would not be compatible with online users' right to freedom of expression and information pursuant to Article 11 of the Charter. They also carry risks for the rights to private life and protection of personal data of other persons under Articles 7 and 8 of the Charter. The impact of enhanced use of automated means and artificial intelligence software, encouraged by the proposal, would significantly impact on the rights of freedom of expression and information and non-discriminatory treatment of online users, also due to the limited reliability of such tools.

The EU legislator should consider deleting Article 6 (1) obliging hosting service providers to apply proactive measures. A relevant recital should instead refer to the positive obligation of the Member States to secure the effective exercise of fundamental rights and prevent fundamental rights violations, including by providing necessary guidance to hosting services providers to ensure that their content restricting polices set out in the general terms and conditions pay due regard to the relevant human rights standards; and underline that the effectiveness of software used to detect terrorist content should be adequately tested, especially from a fundamental rights perspective.

The EU legislator should clarify in Article 6 (2) that the provision aims at preventing the re-appearing of content identical to that previously identified as terrorist, and removed on the basis of a removal order. Furthermore, it should ensure by amending Recital (19) that the proposal does not permit any conflict with EU law, namely by allowing for a derogation from the prohibition of general monitoring obligation, as enshrined in Article 15 of the E-Commerce Directive.

At the same time, the EU legislator should also clarify in Recital (18) that Article 6 (2) should not be interpreted as requiring any hosting service provider to whom a removal order had been addressed to introduce proactive measures, and that the competent authority referred to in Article 17 (1) (c) should take into account the level of exposure of the host service providers to terrorist content.

FRA Opinion 11: Ensuring the right to an effective remedy for hosting service providers against decisions imposing additional proactive measures

The proposal establishes in Article 6 (4) that the competent authority can issue a decision requiring hosting service providers to take specific additional proactive measures on a mandatory basis. At the same time, it only provides for a review by the same competent authority, without requiring that such review should be conducted by a court, contrary to the minimum requirements for an effective remedy under Article 47 of the Charter.

The EU legislator should ensure the right to an effective remedy for hosting service providers against the mandatory imposition of additional proactive measures by amending Article 6 (5) to state that decisions taken pursuant to Article 6(4) shall be subject to review by a court.

Introduction

This Opinion by the European Union Agency for Fundamental Rights (FRA) aims to inform the European Parliament's position on the legislative proposal for a Regulation on preventing the dissemination of terrorist content online, presented by the European Commission on 12 September 2018.[1] Throughout the text, this FRA Opinion refers to the legislative text using the wording "the proposal" or "the proposed Regulation". According to the Explanatory Memorandum to the proposal, terrorists "misuse the internet to groom and recruit supporters, to prepare and facilitate terrorist activity, to glorify in their atrocities and urge others to follow suit."[2] The impact assessment accompanying the proposal points out that availability of online terrorist content can accelerate radicalisation, recruit terrorist supporters and facilitate or instruct terrorist activity.[3]

The proposed Regulation follows a set of recently adopted voluntary measures. It builds on the work of the EU Internet Forum, launched in December 2015 as a framework of voluntary cooperation between Member States and representatives of major internet companies to detect and address online terrorist content. The proposal also operationalises the Commission's Communication on tackling illegal content online, towards enhanced responsibility of online platforms.[4] Finally, it aims to transform into legally binding provisions some of the elements in the Commission Recommendation on measures to effectively tackle illegal content online, which sets up a voluntary framework of action for internet intermediaries.[5]

According to Recital (1) of the proposal, by preventing the misuse of hosting services for terrorist purposes, the proposed Regulation aims to ensure the smooth functioning of the digital single market in an open and democratic society. The proposal contains a definition of "terrorist content" in Article 2 (5) that is directly linked to the definition of terrorist offences set out in Directive (EU) 2017/541 on combating terrorism (Terrorism Directive).[6]

The proposal introduces three specific measures for detecting and removing terrorist content from online platforms. Each requires a different type of action from the hosting service providers:

- Removal orders issued by a national competent authority, oblige hosting service providers to remove the content identified in the order or disable access to it within one hour from its receipt (Article 4).

---

1 European Commission (2018), *Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online*, 2018/0329(COD), COM(2018) 640 final, Brussels, 12 September 2018.

2 Explanatory Memorandum to the proposal, p. 1.

3 European Commission (2018), *Commission Staff Working Document - Impact Assessment Accompanying the Document Proposal for a regulation of the European parliament and of the Council on preventing the dissemination of terrorist content online*, SWD(2018) 408 final, Brussels, 12 September 2018, p. 16.

4 European Commission (2017), *Commission's Communication on tackling illegal content online, towards enhanced responsibility of online platforms*, COM(2017) 555 final, Brussels, 28 September 2017.

5 European Commission (2018), *Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online*, C (2018) 1177 final, Brussels, 1 March 2018.

6 European Union (2017), *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 2017 L 88, 31 March 2018.

- Referrals, which alert hosting service providers about the existence of potentially terrorist content on their platform. Referrals do not directly oblige hosting service providers to remove the notified content. However, they require them to assess the compatibility of such content with their own terms of service and decide whether to remove it or to disable access to it (Article 5).
- Proactive measures introduced by hosting service providers to facilitate identification and the removal of terrorist content from their platforms. The proactive measures should include automated means in certain cases (Article 6).

As noted by the European Commission's Impact Assessment accompanying the proposal, the proposed Regulation will have an impact on fundamental rights. The Agency recognises the importance of the overall goal to prevent the misuse of the internet by terrorists and acknowledges the important contribution the proposed Regulation aims to make in this context. However, the Agency also wishes to bring to the attention of the EU legislator several key fundamental rights concerns that the proposal raises.

The proposal is based on a broad concept of what constitutes dissemination of terrorist content online, and transfers a significant share of the responsibility for addressing the issue to private parties. This shift of responsibility is closely related to the choice of the legal basis of Article 114 (approximation of laws for the improvement of the internal market) rather than Article 83 TFEU (judicial cooperation in criminal matters for the definition of criminal offences) or Article 82 TFEU (Judicial cooperation in criminal matters – procedures). It has serious implications for internet users as well as hosting service providers themselves, as it significantly reduces the legal and procedural safeguards accompanying the measures introduced by the proposed Regulation. The introduction of co-regulatory and self-regulatory tools, such as referrals and proactive measures, in conjunction with a general obligation to prevent dissemination of terrorist content and high penalties, will create an incentive for hosting service providers to more actively remove content and employ more automated tools. Such a development would have major implications primarily on freedom of expression and information but also due process principles in general. Against this background, this Opinion examines the potential implications of the proposed Regulation on freedom of expression and information, which is a cornerstone of democratic society. This right, which also includes the freedom to hold opinions and to receive and impart information and ideas, is enshrined in Article 11 (1) of the Charter. Article 13 of the Charter further establishes the right to artistic, scientific and academic freedom, which is deduced primarily from the right to freedom of thought and expression.[7] According to Article 52 (1) of the Charter, any limitation on the exercise of these freedoms must be provided for by law and respect the essence of these rights. Such limitations must only be made if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

As is evident from Article 52 (3) of the Charter and the Court of Justice of the European Union (CJEU) jurisprudence, the meaning and scope of this right are the same as those guaranteed by Article 10 of the European Convention on Human Rights (ECHR)

[7] *Explanations Relating to the Charter of Fundamental Rights,* OJ 2007 C 303, Explanation on Article 13, 14 December 2013, p. 22.

covering the freedom of expression[8] and as interpreted by the European Court of Human Rights (ECtHR). The limitations, which may be imposed on it, may therefore not exceed those provided for in Article 10 (2) of the ECHR, including the interests of national security, territorial integrity and public safety.[9] The objective of the fight against terrorism represents such a legitimate limitation.[10] For example, restrictions on idealising, condoning or commenting positively on terrorist crimes and terrorists are in principle justified.[11] At the same time, manifest incitement to violence, hatred or other forms of intolerance, which negate the actual values of the ECHR and aim at destroying the rights and freedoms of others, are excluded from the protective scope of freedom of expression altogether.[12]

The ECtHR has nevertheless construed this exclusion narrowly, also in the context of potential terrorist content. The jurisprudence requires that safeguards are in place and states that difficulties related to the fight against terrorism do not negate the obligation to ensure freedom of expression; it only permits restrictions that are necessary and proportionate.[13] Legislation outlawing such expressions must avoid excessive interferences with political speech, or public interest debates and criticism of the authorities that should not be restricted.[14] In this regard, the ECtHR regularly reiterated that freedom of expression is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the state or any sector of the population. Such are the demands of pluralism, tolerance and broadmindedness without which there is no "democratic society".[15] The protective scope of freedom of expression extends beyond the content of information also to the means of its dissemination. This is because "any restriction imposed on the means necessarily interferes with the right to receive and impart information".[16] The ECtHR has also specifically acknowledged the important role that the internet plays for the exercise of freedom of expression facilitating dissemination of information and access by the public.[17]

Apart from freedom of expression and information, there are other fundamental rights and freedoms provided for in the Charter which will be considerably impacted upon by the proposed rules. These include the right to respect for private and family life (Article 7) and the right to protection of personal data (Article 8), freedom of thought, conscience and religion (Article 10), freedom of assembly and of association (Article 12), freedom of the arts and science (Article 13), freedom to conduct a business (Article 16), non-discrimination (Article 21), the right to an effective remedy and to a

---

8 CJEU, *Société Neptune Distribution v. Ministre de l'Économie et des Finances*, Case C-157/14, 17 December 2015, para. 65.

9 *Explanations Relating to the Charter of Fundamental Rights,* OJ 2007 C 303, Explanation on Article 11, p. 21.

10 ECtHR, *Leroy v. France,* No. 36109/03, 2 October 2008, para. 36.

11 ECtHR, *Stomakhin v. Russia, No. 52273/07, 9 May 2018*, paras. 89, 99-107; *Bidart v. France,* No. 52363/11, 12 November 2015, paras. 42-43.

12 ECtHR, *Belkacem v. Belgium, No. 34367/14, 27 June 2017, para. 31; Roj TV A/S v. Denmark, No. 24683/14, 17 April 2018, para. 31.*

13 ECtHR, *Stomakhin v.Russia, No. 52273/07, 9 May 2018*, paras. 107, 117; *Belek and Velioğlu v.Turkey, No. 44227/04, 6 October 2015*, para. 25.

14 ECtHR, *Stomakhin v. Russia, No. 52273/07, 9 May 2018*, paras. 89, 99-107, 117; ECtHR, *Bidart v. France*, No. 52363/11, 12 November 2015, paras. 42-43.

15 ECtHR, *Döner and Others v. Turkey,* No. 29994/02, 7 March 2017, para. 98.

16 ECtHR, *Öztürk v. Turkey, No. 22479/93, 28 September 1999*, para. 49.

17 ECtHR, *Delfi AS v. Estonia, No. 64569/09, 16 June 2015*, paras. 110, 133; ECtHR, *Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom,* Nos. 3002/03 and 23676/03, 10 March 2009, para. 27.

fair trial (Article 47 of the Charter) as well as certain other rights that may arise in the particular context of criminal proceedings, such as the right not to be tried or punished twice in criminal proceedings for the same criminal offence (*ne bis in idem* principle, Article 50).

In light of the scope of the European Parliament's request, this Opinion does not cover all of these rights enshrined in the Charter, which is "addressed to the Member States [...] when they are implementing Union law"[18] or "when they act in the scope of EU law".[19] It focuses, in a non-exhaustive manner, on several selected fundamental rights in relation to which the impact of the proposed regime can be expected to be most significant. On issues with specific impact in the field of privacy and data protection, this Opinion is without prejudice to a possible dedicated opinion delivered by the European Data Protection Supervisor.

This FRA Opinion contains 11 individual opinions that relate to the following rights, namely (in the order of the Articles in the Charter):

- the right to respect for private and family life (Article 7 of the Charter);
- the right to protection of personal data (Article 8 of the Charter);
- the freedom of expression and information (Article 11 of the Charter);
- the freedom to conduct a business (Article 16 of the Charter); and
- the right to an effective remedy and to a fair trial (Article 47 of the Charter).

The Opinion is structured around the main fundamental rights implications connected to the scope of the proposed Regulation (definition of the terrorist content and its dissemination) as well as to individual measures proposed (removal orders, referrals and proactive measures). Given that both issues are closely interrelated, all the specific safeguards proposed in this FRA Opinion are intended to be mutually complementary rather than work in isolation.

More specifically and following the order of individual provisions in the proposed Regulation, Chapter 1 looks at the implications of the definition of terrorist content used by the proposal, including its relation to terrorist offences, the question of what constitutes public dissemination, and the need to protect certain forms of expression. Chapter 2 analyses the fundamental rights implications of the proposed mechanism of removal orders, including involving an independent judicial authority, time limit for complying with removal orders, issue of jurisdiction in cross-border cases, the practical availability of remedies for content providers and the issue of retention of removed content. Chapter 3 examines the proposed referral mechanism, including the responsibility for protecting fundamental rights online. Chapter 4 looks at the issue of due diligence of hosting service providers and the right to judicial protection in the context of proactive measures.

---

[18] See Art. 51 of the *Charter of Fundamental Rights of the European Union*, OJ C 326, 26 October 2012; FRA (2018), *Challenges and opportunities for the implementation of the Charter of Fundamental Rights*, FRA Opinion, 4/2018, Vienna, 24 September 2018.

[19] CJEU, *Åklagaren v. Hans Åkerberg Fransson,* Case C-617/10, 26 February 2013, paras. 20-21. See also FRA (2018), *Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level – Guidance*, Luxembourg, Publications Office of the European Union, pp. 17-18; Hancox, E. (2013), 'The Meaning of "Implementing" EU Law under Article 51(1) of the Charter: Åkerberg Fransson', *Common Market Law Review,* Vol. 50, pp. 1411-1432.

1. Enhancing respect for fundamental rights by providing a clear definition of terrorist content and its dissemination

Article 2 of the proposal defines key terms, including "terrorist content" and "dissemination of terrorist content". The definition of terrorist content in paragraph (5) refers to four types of content. It draws on, as acknowledged in Recital (9) and the Explanatory Memorandum to the proposal, definitions of criminal offences in the Terrorism Directive that cover public provocation to commit a terrorist offence, recruitment and providing training for terrorism.[20] The formulations used by the proposal to define the different types of content are however broader than those used in the Terrorism Directive. In addition, the dissemination of terrorist content in paragraph (6) is defined by means of its availability to third parties rather than public availability, which is the approach of the Terrorism Directive.

This Chapter deals with the impact of the proposed definitions on the right to freedom of expression and information (Article 11 of the Charter). It also takes into account potential implications of the proposal on content disseminated for specific purposes, such as those of an educational, journalistic or research nature. Other rights affected by the proposal, especially the right to private life (Article 7 of the Charter), will also be touched upon.

Given the relevance of the definitions for the overall scope of the Regulation and the measures envisaged therein (namely removal orders, proactive measures, referrals), observations in the subsequent Chapters of this Opinion should be read in conjunction with the findings of this Chapter.

1.1 Enhancing the foreseeability and clarity of the definition of terrorist content

According to the jurisprudence of the ECtHR, the definition of "terrorist content" should be construed as strictly as possible. It should only refer to forms of expression that manifestly incite, glorify or justify violence, hatred or other forms of intolerance relating to terrorist activities.[21] Such expressions must go beyond a mere declaration of sympathy.[22] In accordance with the case law, 'terrorist content' should be assessed in light of the context and circumstances under which it is disseminated, taking into account its possible impact, the means of its dissemination, the authors and their public influence.[23] Similarly, the UN Human Rights Committee emphasised that counter-terrorism measures should not lead to unnecessary or disproportionate interference with the right to freedom of expression.[24]

The definition of types of content considered to be "terrorist" in Article 2 (5) of the proposal is based on formulations in the Terrorism Directive which are conceived as elements of specific criminal offences. This means that the broad definitions in the

[20] Explanatory Memorandum to the proposal, p. 3.

[21] ECtHR, *Roj TV A/S v. Denmark, No. 24683/14, 17 April 2018,* paras. 46-48; *Hizb Ut-Tahrir and Others v. Germany, No. 31098/08, 12 June 2012,* paras. 73-74, 78.

[22] *Ibid*.

[23] ECtHR, *Stomakhin v.Russia, No. 52273/07, 9 May 2018*, paras. 93, 131; *Bidart v. France, No. 52363/11, 12 November 2015*, paras. 35, 45; *M'Bala M'Bala v. France, No. 25239/13, 20 October 2014*, paras. 37-39.

[24] United Nations (2011), *General Comment no. 34 Article 19: Freedom of Opinion and Expression*, para. 46.

Terrorism Directive – such as that of public provocation to commit a terrorist offence in Article 5 of the Terrorism Directive which serves as a basis for Article 2 (5) (a) and includes the term "glorification" [25] – are envisaged to be further refined when the Directive in transposed into national law and applied in criminal proceedings. Here the content would be assessed together with all other relevant circumstances of the case. The full set of specific fair trial guarantees would also apply.

This is not the case of the proposed Regulation. The definitions will be used in the context of different non-criminal measures (removal orders, referrals and proactive measures) applied by different entities including private companies. While these entities will still have to take into account the overall context in order to not to remove content that is actually legal (e.g. disseminated for educational, journalistic or research purposes, see Section 1.3), the evidentiary situation and the presence of safeguards will differ considerably from that for which the definitions in the Terrorism Directive were conceived. In light of the particular risk for the freedom of expression and information, this would require refining the definition to cases where the terrorist nature of the content is manifest.

Furthermore, the definition of terrorist content in the proposal is even broader in some aspects than the definitions laid down in the Terrorism Directive.

The most ambiguous description of terrorist content is contained in Article 2 (5) (b) of the proposal. This covers information "encouraging the contribution to terrorist offences". Such conduct does not seem to accord with any specific offence under the Terrorism Directive. It would therefore either overlap with other types of content or expand the definition of terrorist content beyond what corresponds strictly to offences criminalised under the Terrorism Directive. In addition, the term "encouraging" is vague and does not necessarily correspond to a manifest form of expression inciting to commit a terrorist act or support terrorist activities. Rather, it is susceptible to varying interpretations based on subjective evaluations. This makes it particularly likely to result in disproportionate interferences with the freedom of expression, as guaranteed by Article 11 of the Charter.

Article 2 (5) (c) includes in its scope, the promotion of "activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541". This formulation is broader than its counterpart, in the Terrorism Directive, namely Article 6 on recruitment for terrorism in conjunction with Article 4 (b) which covers participation in a terrorist group. Article 4 (b) of the Terrorism Directive provides a more concrete definition of participation by specifically including "supplying information or material resources" or "funding". It also requires "knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group". The proposal in opposition, lacks these concrete elements delineating participation in a terrorist group. Notably, the open-ended reference to "support" in proposed Article 2 (5) (c) may result in application to content that appears to support the same political or other aims as those of a terrorist group, without the content provider having expressed the slightest sympathy for the group or its terrorist tactics. This could impact, for example, on peaceful political campaigning for self-determination or secession, or other contentious political issues.

[25] United Nations (2018), *Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, OL OTH 71/2018, 7 December 2018, p. 3.

The proposal also includes in its Article 2 (5) (d) information that is "instructing on methods or techniques for the purpose of committing terrorist offences." Again here, the proposal deviates from the wording of the Terrorism Directive by providing a broader and more ambiguous definition of terrorist content. Its application, particularly outside the framework of a criminal trial, may therefore significantly increase the likelihood of capturing also technical, marketing or training materials which are not related to terrorism. The proposal does not define what can be considered as a "method" or "technique" for committing terrorist offences and is thereby open to various interpretations as any type of behaviour can fall under a subjective assessment of this article. On the contrary, the Terrorism Directive in its equivalent provisions provides for a stricter and more precisely worded formulation. Its Articles 7 and 8 read: "instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques, for the purpose of committing, or contributing to the commission of, one of the [terrorist offences pursuant to the Directive]".

FRA Opinion 1

The definition of terrorist content in the proposal draws on definitions of terrorist offences under Directive (EU) 2017/541 (Terrorism Directive), which are however construed for the purposes of criminal proceedings. Furthermore, the proposal deviates from the Directive in important aspects. Article 2 (5) (c) referring to "promoting the activities of a terrorist group"; (d) referring to "instructing on methods or techniques for the purpose of committing terrorist offences"; and, in particular, (b) referring to "encouraging the contribution to terrorist offences". These all potentially broaden the concept of terrorist content beyond that foreseen by the Terrorism Directive. This gives rise to a risk of unlawful interference with fundamental rights, in particular the right to freedom of expression guaranteed in Article 11 of the Charter.

The EU legislator should ensure that the proposed Regulation will only apply to content which would manifestly fall under the scope of the Terrorism Directive. For this reason, the EU legislator should consider amending proposed Article 2 (5) as follows:

"(5) 'terrorist content' means information which, in a manifest manner:

> ***(a) incites or advocates, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;***
>
> ***(b) promotes the activities of a terrorist group, in particular by inciting, soliciting or advocating persons or a group of persons to participate in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way; or***
>
> ***(c) provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques, for the purpose of committing, or contributing to the commission of, terrorist offences."***

1.2 Clearly limiting the scope of the proposal to content disseminated in the public

Article 1 (1) (a) of the proposal defines the subject matter and scope of the new Regulation which establishes "rules on duties of care to be applied by hosting service

providers in order to prevent the dissemination of terrorist content through their services". Article 2 (1) of the proposal defines 'hosting service provider' as an entity making "the information stored available to the public". Proposed Article 2 (6) defines "dissemination of terrorist content" as the means of making terrorist content available to third parties, in a manner that covers information society services such as social media platforms, video streaming services, video, image and audio sharing services, file sharing and other cloud services. According to Recital (10), any service in which information is stored at the request of the recipient of the service, or made available to a third party, falls under the scope of the proposal.

Such a wide formulation could therefore be interpreted to include service providers that offer services not available to the public. For example, content stored on cloud services that do not make information publicly available, but allow for the sharing of uploaded content with another user, or a restricted number of users could be construed as making content "available to third parties." This wording therefore arguably lacks sufficient clarity as to what type of service providers it covers. It could well apply to business-to-business cloud providers, or any cloud-based service allowing users to collaborate with a limited private set of users. It could also be applied to providers of VoIP (Voice over Internet Protocol) or electronic messaging services, including emails and internet texting as such 'sound recordings' are made available to third parties.

The possibility of this broad application, seems to fall short of the objective echoed in Recital (7) of the proposal which ensures that any interference in the freedom of expression and information is "strictly targeted." Similarly, it does not meet the requirement of establishing "appropriate and robust safeguards to ensure protection of the fundamental rights". Outlawing any form of expression, either as a derogation from the freedom of expression or as a restriction to it, requires an examination of the content in light of its context and circumstances under which it was made. It requires an assessment of its potential to lead to harmful consequences, and, in particular, of its influence and means of dissemination to the wider public.[26] Therefore, any content not available in the public sphere cannot logically be the subject to this assessment, which is required to render it unlawful in and of itself. Any measure aimed at content distributed privately, would constitute an unprecedented restriction and interference with the rights of freedom of expression under Article 11, and private life and correspondence under Article 7 of the Charter.

Moreover, this approach could result in measures being taken on a general and indiscriminate basis even against people for whom there is no objective evidence that they participate in, or otherwise support, terrorist activities. In this context, it should be underlined that the relevant provisions of the Terrorism Directive are restricted solely to content disseminated (distributed or otherwise made available) to the public, as the purposes of its measures "on the internet is to remove online content constituting a public provocation to commit a terrorist offence at its source."[27]

FRA Opinion 2

Unlike the Terrorism Directive which covers content disseminated to the "public", the proposal applies to any content that becomes "available to third parties". This broad formulation means that the Regulation could be interpreted as applying to private communication – emails, private messaging and cloud infrastructure services – which

[26] ECtHR, *Stomakhin v. Russia*, *No. 52273/07, 9 May 2018,* paras. 93, 131; ECtHR, *Bidart v. France,* No. 52363/11, paras. 35, 45; ECtHR, *Roj TV A/S v. Denmark*, No. 24683/14, 17 April 2018, para. 47.

[27] Directive (EU) 2017/541, Recitals (22) and (23), Article 21.

would represent a disproportionate and unjustified interference with the freedom of expression and information under Article 11 of the Charter and the right to private and family life under Article 7 of the Charter.

The EU legislator should ensure that the proposed Regulation does not apply to expression which does not enter the public domain, disproportionately interfering with the rights to freedom of expression and private life and correspondence of internet users at large. Accordingly, the EU legislator should consider:

- ***replacing in Recital (10) the term "third parties" with "the public";***
- ***replacing in Article 2 (1) and (6) the term "third parties" with "the public";***
- ***adding the term "public" before "dissemination" in Article 1 (1) (a).***

1.3 Excluding certain forms of expression from the scope of the proposal

Recital (9) of the proposal underlines that "[c]ontent disseminated for educational, journalistic or research purposes should be adequately protected. Furthermore, the expression of radical, polemic or controversial views in the public debate on sensitive political questions should not be considered terrorist content". This acknowledgement reflects ECtHR jurisprudence which requires particular caution to such protected forms of speech and expression, including also artistic expression.[28] In particular, the jurisprudence recognises the right of journalists to report or comment on such unlawful speech or content, provided they distance themselves and do not espouse it.[29] Extensive restrictions on journalists "for assisting in the dissemination of statements made by another person in an interview would seriously hamper the contribution of the press to discussion of matters of public interest and should not be envisaged unless there are particularly strong reasons for doing so".[30] In addition, the Committee of Ministers of the Council of Europe has recommended to avoid the universal and general blocking of illegal content for users who justifiably demonstrate a legitimate interest or need to access such content under exceptional circumstances, particularly for research purposes.[31]

However, Recital (9) of the proposal is not reflected in the operative provisions by providing an exception for such purposes. Indeed, there may well be instances whereby content that could be classified as 'terrorist' needs to be disseminated for journalistic, research, educational or other similar purposes. For example, it is usual for journalists to report or disseminate parts of content produced by terrorists, usually in a redacted or further processed form, to inform the public. Appropriate dissemination of such content can have a dissuasive effect on terrorist activities by informing the public of their criminal acts and reinforcing public rejection of terrorist activities. The same applies for research institutions and individuals studying terrorist activities and providing findings that can inform counter-terrorism policies, as well as for many forms of literary or artistic expression.

---

28 ECtHR, *M'Bala M'Bala v. France, No. 25239/13, 20 October 2014,* para. 31.

29 ECtHR, *Roj TV A/S v. Denmark*, No. 24683/14, para. 42; ECtHR, *Jersild v. Denmark, No. 15890/89*, 23 September 1994, paras. 33-36.

30 ECtHR, *Jersild v. Denmark, No. 15890/89*, 23 September 1994, para. 35.

31 Council of Europe (2008), *Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on Measures to promote the respect for freedom of expression and information with regard to Internet filters*, para. III (vi).

The Terrorism Directive also recognises the need to exclude such content in Recitals (11) and (40) rather than in the operative provisions. This can be, however, explained by the difference between the two instruments. The Terrorism Directive is applied during criminal proceedings, where such issues would be considered in relation to intent (an element not required by the proposal); furthermore the different legal nature of directives foresees that detailed rules are established as part of the transposition into the national legal framework. As a regulation, the proposed legal instrument would not allow for national legislators to introduce such exception clauses into their national legislation.

In fact, national legislations usually require such exceptions. For example, the German legislator included similar exceptions in the Criminal Code that apply to offences of disseminating propaganda material of unconstitutional organisations; encouraging the commission of a serious violent offence endangering the state; incitement to hatred; and attempting to cause the commission of offences by means of publication.[32]

Expressing this important principle only in a recital cannot itself ensure that such protected forms of expression are adequately respected. It also cannot ensure that content which appears at first unlawful, can be used for legitimate purposes, notably journalism or research.

FRA Opinion 3

The preamble of the proposal acknowledges the need to ensure that certain protected forms of expression are respected. Nevertheless, the proposal lacks provisions that would explicitly oblige competent authorities and courts to exclude dissemination of content for legitimate purposes, notably informing the public of matters of public interest and promoting education, academic and scientific research, or literary or artistic expression.

The EU legislator should ensure that forms of expression such as journalistic, academic and artistic expression are adequately protected, such as by considering introducing in Article 1 of the proposal a new paragraph (3), in line with Recital (9), providing that "Content disseminated for educational, journalistic, artistic or research purposes or awareness raising activities against terrorism is excluded."

[32] Germany, Criminal Code (*Strafgesetzbuch*), 13 November 1998, Article 86 (3) in conjunction with Articles 86, 91, 130 and 130a, respectively.

2 Strengthening fundamental rights safeguards on removal orders

Article 4 of the proposal provides for the power of a competent authority of any Member State to issue a decision requiring the hosting service provider to remove or disable access to terrorist content. These orders are addressed to hosting service providers who are under the obligation to comply within one hour. This Chapter examines the main elements of the removal order mechanism. It looks at the nature of the issuing body and a lack of a clear requirement for independent and impartial judicial oversight, including cross-border removal orders; the mandatory nature of the order; the one-hour limit to remove or block access to content identified as terrorist; the need to provide sufficient information to content providers and the obligation to preserve content that has been removed or disabled.

The Chapter addresses fundamental rights challenges in the context of freedom of expression and information under Article 11 and freedom to conduct a business under Article 16 of the Charter; the right to respect for private life under Article 7 and the right to protection of personal data under Article 8 of the Charter, as well as the right to an effective remedy to potential violations of these rights under Article 47 of the Charter.

2.1 Safeguarding fundamental rights through effective judicial supervision

According to Article 11 of the Charter, freedom of expression and information includes the freedom to hold opinions and to receive and impart information and ideas without interference by a public authority. As underlined in the Introduction, incitement to violence is excluded from the protective scope of the freedom of expression.[33] The ECtHR has nevertheless construed this exclusion narrowly, also in the context of potential terrorist content. It requires that safeguards are in place and states that difficulties related to the fight against terrorism do not negate the obligation to ensure freedom of expression; and only restrictions that are necessary and proportionate should be applied.[34]

The ECtHR has emphasised the importance of judicial intervention in cases related to the freedom of expression to provide a genuine safeguard against abuse.[35] In *Ekin v. France*, the ECtHR ruled that judicial review of administrative publishing bans which only took place *ex post* and required an application to court, together with an excessive length of such review proceedings, provided insufficient guarantees against abuse.[36] Also when assessing the nature of online content and the need for its removal, an independent judicial authority would be best placed to make an impartial decision to meet public security needs without violating fundamental rights. This is of particular importance for measures that have an immediate effect on fundamental rights while a subsequent remedy may have limited restorative effect, such as prolonged proceedings eventually leading to the restoration of online content.[37]

---

[33] ECtHR, *Belkacem v. Belgium*, No. 34367/14, 27 June 2017.
[34] ECtHR, *Perinçek v. Switzerland [GC], No. 27510/08, 15 October 2015*, para. 197.
[35] See for example ECtHR, *Bidart v. France,* No. 52363/11, 12 November 2015, paras. 38-41.
[36] ECtHR, *Association Ekin v. France, No. 39288/98, 17 July 2001*, para 61.
[37] See e.g. Kuczerawy, A., *The Proposed Regulation on preventing the dissemination of terrorist content online: safeguards and risks for freedom of expression*, Center for Democracy and Technology, 5 December 2018, p. 10.

The proposal does not require any involvement of an independent judicial authority in the issuing of, or prior to the execution of, removal orders, i.e. before the interference with fundamental rights takes place, to assess its necessity and proportionality. In the absence of a definition of the 'competent authorities', Recital (13) merely states that "Member States should remain free as to the choice of the competent authorities allowing them to designate administrative, law enforcement or judicial authorities with that task." The Explanatory Memorandum to the proposal underlines this by stating that the removal order can be issued "as an administrative or judicial decision by a competent authority in a Member State."[38]

At the same time, none of the parties involved have a realistic opportunity to initiate a review of the legality of the order and its interference with fundamental rights prior to the removal of the content.

As regards the content providers, whose freedom of expression and information is primarily affected by the removal, the proposal foresees only notifying the removal or disabling of access that has already taken place, further limited in Article 11 (see also Section 2.4). While excluding the content provider at this stage might be legitimate in light of the nature of the public interest involved, it reinforces the need for alternative safeguards.

The need to protect individuals' fundamental rights without alerting them to the actual existence of a security measure in order not to jeopardise a legitimate public interest is not unique. A parallel could be drawn, for example, with the use of surveillance and communication interception measures by intelligence authorities outside of the law enforcement context. In such cases, the ECtHR acknowledged that the very nature and logic of secret surveillance measures often means that in practice, individuals are simply not able to effectively seek a remedy of their own accord or to take a direct part in any review proceedings. In such cases, it is therefore essential to provide some form of judicial supervision in order to safeguard adequate and equivalent guarantees for the rights of individuals.[39]

Hosting service providers are also not foreseen by the proposal to make their own assessment of the removal orders and, where relevant, contest them. Instead, the proposal foresees their automatic compliance with the measure. The Explanatory Memorandum states that such orders "would not necessarily require an assessment on the part of the hosting service providers".[40] The Impact Assessment makes the same argument in relation to costs, stating that costs and burdens for hosting service providers would be mitigated because the competent authority would assess the content and providers would not need to invest resources to make the assessment themselves.[41]

The only exceptions from the mandatory nature of the removal orders foreseen by the proposal relate to *force majeure* or other *de facto* impossibility not attributable to the hosting service provider (Article 4 (7)), or manifest errors or insufficient information in the removal order itself (Article 4 (8)). Such "manifest errors" of removal orders

---

38 Explanatory Memorandum to the proposal, p. 4.

39 ECtHR, *Roman Zakharov v. Russia [GC]*, No. 47143/06, 5 December 2015; ECtHR, *Szabo and Vissy v. Hungary*, No. 37138/14, 12 January 2016.

40 Explanatory Memorandum to the proposal, p. 7.

41 European Commission (2018), *Commission Staff Working Document – Impact Assessment Accompanying the Document Proposal for a regulation of the European parliament and of the Council on preventing the dissemination of terrorist content online*, SWD(2018) 408 final, Brussels, 12 September 2018, pp. 42 and 103.

apparently do not extend to the potential erroneous assessment of the content as "terrorist" by the competent authority, as hosting service providers will not be provided with sufficient information about the assessment. Although Article 4 (3) (b) requires the authority to state why the content is considered terrorist, this can be limited to referring to one of the broadly conceived categories listed in Article 2 (5) (see Section 1.1). The competent authority has the obligation to give a detailed statement of reasons, only in cases where the hosting service provider or the content provider so request. Pursuant to proposed Article 4 (4), this does not, however, suspend the one-hour limit for complying with the removal order.

This means that even when hosting service providers consider that the right of their users to freedom of expression and information or their own right to conduct a business (see Section 2.2) would be disproportionately affected by complying with the removal order, they would not be able to effectively contest the removal order.

Given this degree of automatism to the implementation of removal orders and the potential level of interference with fundamental rights that issuing of removal orders entails, the measure should be conceived in a manner that directly integrates the supervision by a judicial authority. Ensuring that every competent authority issuing removal orders is of judicial nature would provide the most adequate and effective guarantees against rights violations. If this option is not feasible in the context of the given national legal order, speedy judicial review should take place immediately after the removal order is issued and ideally, before the content is actually removed or, shortly thereafter. In such cases, the proposal would need to establish a procedure for restoring the content in situations where the hosting service provider receives a negative decision of the independent judicial authority after the content has already been removed or access to it disabled.

FRA Opinion 4

Removal orders as regulated in Article 4 of the proposal require hosting service providers to remove or disable access to content identified by the competent authority as terrorist. The proposal does not guarantee any type of involvement of an independent judicial authority in the adoption or prior to the execution of the removal order. At the same time, neither the content provider nor the hosting service provider are afforded a mechanism to effectively challenge the order before the removal is carried out. Combined with the limitations on access to an effective remedy once the removal has already taken place, this offers insufficient protection to the rights at stake, in particular freedom of expression and information and freedom to conduct a business under Articles 11 and 16 of the Charter.

In order to ensure that removal orders are always based on an independent and impartial assessment, the EU legislator should prescribe that the competent authority responsible for issuing removal orders be an independent judicial authority.

Alternatively, the EU legislator could consider:

- ***amending Article 4 (1) by stating that where the competent authority is not a judicial authority, or where the removal order is not based on a judicial authority's decision, the removal order addressed to the hosting service provider shall be at the same time submitted for review to an independent judicial authority determined in accordance with national law; this judicial authority shall notify the competent authority and the hosting service***

provider of its decision within twenty-four (24) hours from the receipt of the removal order;

- ***adding in Article 4 (2) that where the judicial authority conducting a review pursuant to paragraph (1) issues a decision that does not confirm the removal order's legality, the competent authority shall ensure the immediate restoration of such content, provided it has already been removed or access to it disabled.***

2.2 Avoiding disproportionate impact on the freedom to conduct a business

From the perspective of the hosting service providers, the introduction of removal orders as set out in the proposed Regulation would represent an interference with the freedom to conduct a business, as recognised in Article 16 of the Charter.[42]

This Charter right is based on CJEU case law which has recognised the freedom to exercise an economic or commercial activity, the freedom of contract and free competition. This right is to be exercised with respect for Union law and national legislation. As a non-absolute right, it may be subject to restrictions in line with Article 52 (1) of the Charter where they correspond to objectives of public interest pursued by the EU and (do) not constitute, in relation to the aim pursued, a disproportionate and intolerable interference, impairing the very substance of the rights thus guaranteed. The CJEU has already established that the fight against terrorism constitutes such an objective.[43] The obligation to comply with removal orders nevertheless needs to strike fair a balance between the right to conduct a business and the legitimate aim of combating online terrorist content in order to ensure that the limitations on the right are not disproportionate.

It is noteworthy that while the Explanatory Memorandum identifies the freedom to conduct a business as the key right of the service providers affected by the proposal, it is referenced in Recital (19) relating to proactive measures, but not in the relevant recitals relating to removal orders.

The mandatory nature of removal orders (see also Section 2.1) is underlined by the exposure of hosting service providers to penalties in case of non-compliance. Such sanctions are envisaged in Article 18 of the proposal, but are further undefined and left at the discretion of Member States. This would expose the hosting service providers to a considerable degree of uncertainty.

Hosting service providers are expected to bear the costs of compliance with removal orders. These include, for example, costs incurred due to technical modalities that will need to be put in place to remove or block the content and receive the orders. They also include the costs for necessary personnel to address the orders (i.e. extra working time or additional personnel). This interference with the right to conduct a business is specifically acknowledged in the Impact Assessment accompanying the proposal, in

[42] For a further analysis of this right, see FRA (2015), *Freedom to conduct a business: exploring the dimensions of a fundamental right*, Luxembourg, Publications Office of the European Union.

[43] CJEU, *Kadi and Al Barakaat International Foundation v Council and Commission of the European Communities*, Cases C-402/05 P and C-415/05 P, 3 September 2008, para. 363; CJEU, *Al-Aqsa v Council and Pays-Bas / Al-Aqsa*, Case C-539/10 P, 15 November 2012, para. 130; CJEU, *Digital Rights Ireland and Seitlinger and Others*, Case C-293/12, 8 April 2014, para. 42.

particular with regard to the one-hour rule. It is specifically noted that "the major costs are those related to the application of the one-hour deadline for removal order".[44]

The one-hour limit is proposed, according to Recital (13), due to the "speed at which terrorist content is disseminated across online services." It will require all relevant businesses, irrespectively of their size, to have in place mechanisms allowing them to comply with removal orders on a 24/7 basis. This will be particularly burdensome for small and medium-sized enterprises. According to the available data in Europe almost 10,000 hosting service providers are small, medium or micro enterprises (the latter being half of the total). Also, nearly 70% of Europol referrals in 2018 were addressed to such enterprises.[45] Most of these follow daily schedules according to the time zone of the state where they are located. Complying with such orders outside their working hours and days will require even micro enterprises to employ staff that work on a 24/7 basis. For online platforms or applications – especially the latter – the technical specificities required may even outweigh the costs incurred to set up the platform initially. The one-hour rule therefore carries a serious risk of undermining disproportionately the freedom to conduct a business, especially for small, medium or micro enterprises and individual entrepreneurs. This potentially puts these enterprises at a competitive disadvantage due to the major changes in their *modus operandi*, and the necessary investments, required to comply with the obligation.

In addition, in order to reduce the associated costs and ensure compliance outside regular working hours, some enterprises may seek to automate this process to the extent possible, potentially complying even with those removal orders that contain manifest errors, i.e. where it would otherwise be possible and legitimate to postpone the removal until the competent authority provides a clarification. This could further increase the risk of removing legitimate content and a violation of the freedom of expression and information.

Other than the general reference in Recital (13), the proposal does not further elaborate on the proportionality of the one-hour limit necessary to attain the objectives of the proposal. It also does not provide arguments to support the harmonising nature of the proposed limit. Available evidence from the Council of Europe concludes that such orders require action on the part of hosting service providers usually within 24 hours or more.[46] For EU Member States, the time limits vary between 24 hours (e.g. France) and two working days (e.g. UK). In some Member States, a general period may be shortened in case of manifestly illegal content (e.g. from seven days to 24 hours in Germany).[47]

It is conceivable that there may indeed be specific cases where content is not only manifestly illegal but also poses an imminent threat, such as inciting the commission of a terrorist attack in relation to an event that will take place shortly (e.g. a specific concert or a sports event). In such exceptional cases, it may be legitimate for the

---

[44] European Commission (2018), *Commission Staff Working Document – Impact Assessment Accompanying the Document Proposal for a regulation of the European parliament and of the Council on preventing the dissemination of terrorist content online*, SWD(2018) 408 final, Brussels, 12 September 2018, pp. 36-37, also p. 103.

[45] *Ibid*, p. 36.

[46] Council of Europe (2016*), Comparative study on blocking, filtering and take-down of illegal internet content, Document and Publications Production Department, Council of Europe, 15 April 2016*, p. 16.

[47] European Commission (2018), *Commission Staff Working Document – Impact Assessment Accompanying the Document Proposal for a regulation of the European parliament and of the Council on preventing the dissemination of terrorist content online*, SWD(2018) 408 final, Brussels, 12 September, p. 116 et seq.

competent authority to have the possibility to apply shorter time limits, possibly as short as one hour. When deciding on the concrete deadline, the competent authority would nevertheless need to take into account the time zone, working days and hours of the hosting service provider addressed by the measure.

Outside these exceptional cases, in light of the existing standards described above as well as the impact on the freedom to conduct a business and the freedom of expression, the proposed time limit does not appear to be proportionate to the intended aim. This is especially true if applied to all types of businesses (including, for example, smaller businesses that provide services to a smaller number of users where the content is not publicly available to larger groups of persons) and all types of content, irrespectively of the content's potential to cause an imminent threat. It would therefore appear proportionate to introduce a harmonised time limit aligned with those currently applied by Member States, such as 24 hours.

FRA Opinion 5

The proposed rules for the implementation of removal orders will have considerable implications on the operation of hosting service providers. The time limit of one hour to comply with the removal order, which applies to all host service providers and any content – irrespective of whether it poses an imminent threat – is significantly stricter than the current practice among EU Member States. It may represent a disproportionate restriction to the freedom to conduct a business under Article 16 of the Charter, especially with regard to smaller businesses. It could also lead to automation in the processing of removal orders, with a further negative impact also on the freedom of expression and information of users under Article 11 of the Charter.

In order to avoid disproportionate impact of removal orders on the operation of hosting service providers and the risk of further negative effects on fundamental rights, the EU legislator should consider:

- ***amending Article 4 (2) of the proposal as follows: "Hosting service providers shall remove terrorist content or disable access to it within twenty-four (24) hours from receipt of the removal order. In exceptional circumstances where the competent authority stipulates in the removal order that the particular content poses an imminent threat, hosting service providers shall remove terrorist content or disable access to it within a period shorter than twenty-four (24) hours from receipt of the removal order. The period shall be specifically defined by the competent authority in the removal order; and it cannot be less than one hour from receipt of the removal order, taking into account the time zone, working days and hours of the addressee hosting service provider."***
- ***amending Article 4 (4) of the proposal to provide that the detailed statement of reasons should contain, where applicable, also the reasons which require removing of the content or blocking access to it within less than twenty-four hours.***

2.3 Ensuring additional safeguards in cross-border removal orders by involving the authorities and courts of the host Member State

The proposed Regulation sets out a system according to which a removal order addressed to the hosting service provider can be issued by a competent authority of any EU Member State. This is not necessarily the Member State in which the provider

has its main establishment or in which it has designated a legal representative (Article 4 (5) and Recital (34) of the proposal). This direct interaction between a service provider and the issuing Member State without any involvement of the host Member State, continues also in the context of actual enforcement of the removal order. Indeed, where an authority of another Member State has issued a removal order, that Member State has jurisdiction to take coercive measures according to its national law in order to enforce the removal order (Article 15 (3)). Also, the possibility for hosting service providers (as well as content providers) to contest the removal orders can only take place before the court of the Member State whose authorities issued the removal order. No one can challenge a removal order in front of a court in the Member State of the service provider's establishment (or in which it has designated a legal representative), the reason being that the authorities of this state are not involved in the procedure leading up to a binding removal order.

This legal construction raises concerns from the fundamental rights perspective, in particular in light of the well-established case law of the ECtHR on the state responsibility and effective remedies. According to Article 1 of the ECHR, Contracting States shall secure to everyone within their jurisdiction the rights and freedoms set out in the ECHR. This introduces a very clear rule on the responsibility of states for what happens within their jurisdiction. It means that Article 13 of the ECHR read in light of Article 1 of the ECHR gives individuals a right to an effective remedy in the territory where they claim that their rights were abused without having to turn to another Contracting State. In the Charter, the right to an effective remedy is encompassed under Article 47. Article 52 (3) of the Charter confirms that, where Charter rights correspond to ECHR rights, the meaning and scope of those rights are the same (although more extensive protection can be provided). A smooth functioning of the digital single market in an open and democratic society, which represents the legal basis for the proposal, should not in any way undermine these obligations.

Applying these principles as well as the relevant ECtHR case law standards to the situation covered by the draft Regulation, the Member State which did not issue a removal order but in which the provider has its main establishment (or in which it has designated a legal representative) is fully accountable under the ECHR for infringements of the rights of persons within its jurisdiction "as a result of acts performed by foreign officials with that State's acquiescence or connivance".[48] The ECtHR's findings that a court in the host Member State must be "empowered to conduct a review commensurate with the gravity of any serious allegation of a violation of fundamental rights in the State of origin [issuing Member State], in order to ensure that the protection of those rights is not manifestly deficient" [49] , rules out situations where a service provider in Member State "A" is bound by a removal order issued by an authority of Member State "B" without having any remedy available in their Member State "A".

FRA Opinion 6

In cases of cross-border removal orders, the proposal creates a system in which an order issued by one Member State cannot be challenged in the Member State in which the hosting service provider is established (or in which it has a designated legal representative). In line with the basic principles of territorial jurisdiction and related ECtHR case law, the host Member State must be empowered to review the removal

[48] ECtHR, *Husayn (Abu Zubaydah) v. Poland*, No. 7511/13, 24 July 2014, para. 479.
[49] ECtHR, *Avotiņš v. Latvia*, No. 17502/07, 23 May 2016, para. 114.

order in cases where there are reasonable grounds to believe that fundamental rights are impacted within its own jurisdiction. At the same time, in line with the right to an effective remedy enshrined in Article 19 TEU and Article 47 of the Charter, each natural or legal person has the right to an effective remedy before the competent national tribunal against any of the measures which can adversely affect the rights of that person. Accordingly, the right should include the possibility for hosting service providers and content providers to effectively contest the removal orders before a court of the host Member State, where it is different from the issuing Member State.

The EU legislator should ensure that cross-border removal orders are regulated in a manner which provides sufficient safeguards to the affected fundamental rights, including by providing access to an effective remedy. The EU legislator should address this explicitly in the relevant substantive provisions by:

- ***requiring the issuing Member State to notify competent authorities in the host Member State, alongside the hosting service provider, of the removal order when it is issued;***
- ***introducing additional safeguards to ensure access to an effective remedy, by providing in substantive articles for the possibility of effectively challenging the removal order before a competent court of the host Member State.***

2.4 Providing sufficient information to content providers as a precondition for exercising the right to an effective remedy

Under EU, Council of Europe as well as UN law, the right of access to a court is an important element of access to justice given that courts provide protection against unlawful practices and uphold the rule of law.[50] Article 14 of the International Covenant on Civil and Political Rights (ICCPR) provides for a general guarantee of equality before courts and tribunals that applies regardless of the nature of proceedings before such bodies.[51] Article 13 of the ECHR offers protection to individuals who wish to complain about alleged violations of their rights under the ECHR, by providing for an effective remedy before a national authority. The national authority does not have to be a judicial authority; however, it is accepted that judicial remedies "furnish strong guarantees of independence, access for victims and families, and enforceability of awards in compliance with the requirements of Article 13."[52] Article 47 of the Charter embodies the EU general principle of law whereby Member States must ensure effective protection of an individual's rights arising from Union law, including Charter rights, by providing for an effective remedy before a tribunal.

Article 47 of the Charter requires that remedies shall be effective and have a reasonable prospect of success. The obligation to inform can generally be perceived as a strong safeguard for ensuring the effectiveness of a remedial action, and, ultimately, legal scrutiny by judicial bodies. Effective judicial review presupposes that those affected are able to defend their rights under the best possible conditions. They also have the possibility of deciding, with full knowledge of the relevant facts, whether

[50] See also: FRA (2016), *Handbook on European law relating to access to justice*, p. 26.
[51] UN Human Rights Committee (UN HRC), *General Comment No. 32, Article 14, Right to equality before courts and tribunals and to a fair trial*, 23 August 2007, CCPR/C/GC/32.
[52] ECtHR, *Z and Others v. the United Kingdom [GC], No. 29392/95, 10 May 2001*, para. 110.

there is any point in applying to the courts. Hence, competent authorities are under a duty to inform those affected of the reasons behind the decision.[53]

According to CJEU case law, the review guaranteed by Article 47 of the Charter first requires full knowledge by the individual of the information on which the decision is based. The adversarial principle shall be complied with, so that the individual can decide whether there is an argument to make against the decision. At the same time, for overriding reasons connected to national security, it may prove necessary not to disclose certain information to the individual. However, the court shall be able to review whether the invoked reasons are valid, and the Member States' authority shall prove that the disclosure of the information would compromise national security. There is no presumption that the reasons invoked exist and are valid.[54]

The information obligation of the competent authority under the proposal is limited to the information provided to the hosting service provider in the removal order. According to proposed Article 4 (4), a "detailed statement of reasons" can be requested by the hosting service provider or content provider. This, however, presupposes the existing knowledge of the content provider about the removal. At the same time, the proposal does not establish any obligation to inform the content provider about available legal remedies, as information about possible redress is only provided as part of the removal order which is not communicated to the content provider.

The obligation to inform the content provider is therefore left primarily to the hosting service provider. Recital (26) of the proposal, referencing the need to ensure effective legal protection according to Article 19 TEU and Article 47 of the Charter, states that hosting service providers should make "meaningful information enabling the content provider to contest the decision" available to the content provider. Article 11 (1) of the proposal, however, limits this to information "on the removal or disabling of access". Recital (26) clarifies that this obligation does not necessarily require the content provider to be notified directly but can be fulfilled, for example, by replacing the removed content with a message that the content has been removed or disabled. Further information about the reasons for removal and possibilities to contest the decision is given by the hosting service provider upon request of the content provider. According to proposed Article 11 (3), such information may not be given for reasons of public security, such as the prevention, investigation, detection and prosecution of terrorist offences. This derogation is restricted to the time necessary, not exceeding four weeks.

This situation where the content provider can at different stages and predominantly upon request receive partial information about the decision leading to the removal and the avenues of redress, does not allow individuals to effectively exercise their right to judicial protection. The information necessary for that purpose would include, in particular, the identification of the competent authority issuing the removal order; the competent courts to decide on legal remedies against removal orders and the applicable time limits; the statement of reasons by the competent authority; the Uniform Resource Locator (URL) and any additional information identifying the content referred; the legal basis on which the order was issued and any information about its authenticity. This information is to some extent contained in the removal order.

---

[53] CJEU, *Union nationale des entraîneurs et cadres techniques professionnels du football (Unectef) v. Georges Heylens and Others, C-222/86, 15 October 1987*, para. 15.

[54] CJEU, *ZZ v. Secretary of the State of Home Department*, C-300/11, 4 June 2013, paras. 53-54, 57, 61 and 64.

However, Articles 4 (4) and 11 (2) of the proposal do not secure that the content provider would at any stage of the procedure, even upon request, receive the removal order. Without access to the removal order, the vague information on "possibilities to contest the decision" which should be granted by the host service provider only upon the request of the content provider, does not appear to be sufficient to seek legal remedy.

FRA Opinion 7

The proposal does not ensure that the content provider receives a copy of the removal order, which represents the legal basis for the removal, contains important information not available through other means, and would be necessary to challenge the measure effectively before the courts. Neither does it ensure that the content provider is informed about the available legal remedies against such orders. Therefore, the proposal does not guarantee that content providers have full knowledge of all relevant facts needed to decide whether and on what grounds they will challenge the removal order. As a result, the proposed Regulation does not provide for minimum safeguards ensuring the effectiveness of a remedial action and legal scrutiny by judicial bodies in line with Article 47 of the Charter.

The EU legislator should ensure that the content provider can receive, at the latest after the removal or disabling of access to the content, a copy of the removal order and information about available legal remedies to effectively exercise its right under Article 47 of the Charter. For this reason, the EU legislator should consider amending:

- ***Recital (26) fifth sentence, to state: "Further information about the reasons for the removal, as well as a copy of the removal order and information of the possibilities for the content provider to contest the decision before a court should be given upon request."***
- ***Article 4 (4), to state: "Upon request by the hosting service provider or by the content provider, the competent authority shall provide a copy of the removal order including a detailed statement of reasons, and any information about the available legal remedies to appeal against removal orders before a court, without prejudice to the obligation of the hosting service provider to comply with the removal order within the deadline set out in paragraph 2."***
- ***Article 11 (2) to add the following: "[…] and shall provide him or her with a copy of the removal order issued according to Article 4 upon request."***

2.5 Introducing clear safeguards in relation to preserved content that has been removed or disabled

Article 7 of the proposal requires hosting service providers to preserve removed content and any related data following a removal order. Authorities can then access such data for investigative and prosecutorial purposes. According to Recital (20), these data include subscriber data (e.g. IP address, names and addresses) and access data (date and time of any communications). Access to such data represents an interference with the protection of personal data and the right to private life, enshrined in Articles 7 and 8 of the Charter.[55] Such an interference may be justified and necessary

[55] CJEU, *Digital Rights Ireland and Seitlinger and others [GC], Joined cases C-293/12 and C-594/12, 8 April 2014*, paras. 34-36; CJEU, *Ministerio Fiscal, C-207/16, 2 October 2018*, para. 51.

as it pursues an "objective of general interest", since these data will most probably have probative value for investigative purposes[56] or represent a safeguard in case of erroneous removal (false positives). Nevertheless, the proposed Regulation does not stipulate the conditions of access to data preserved by authorities. Recital (23) merely refers to national law, which will regulate such access and will, therefore, fall within the scope of EU law.[57] In this regard, the CJEU has unequivocally held in *Tele2 Sverige AB*, which concerned access to data retained for criminal purposes that such access must be subject to "*a prior review by a court or an independent administrative body, except in cases of validly established urgency*".[58] Similarly, the lack of this requirement was one of the reasons the CJEU annulled Directive 2006/24/EC (Data Retention Directive)[59] in 2014.[60]

Article 7 of the proposal foresees that the terrorist content and related data are preserved for six months, which can be extended to allow review procedures to be finalised. However, the proposal does not contain a clear requirement of the destruction of the data once this period expires. This creates a danger that data preserved will not be erased and therefore, will be susceptible to abuse, e.g. unauthorised use or access. The ECtHR has established that limited and clearly prescribed rules should regulate both the duration of the storage time of such data, as well as their subsequent destruction.[61] In *Roman Zakharov v. Russia,* the ECtHR held that the contested measure was in breach of the right of privacy because, *inter alia*, it was not sufficiently clear on the storage and destruction of the data collected.[62]

FRA Opinion 8

Article 7 of the proposal envisages that data preserved following removal orders may later be accessed for investigatory or prosecutorial purposes. Nonetheless, it does not require that such access depend upon prior review by a court or independent administrative body. The proposal also does not clearly stipulate the requirement to erase any data preserved following their preservation period. According to the CJEU and ECtHR jurisprudence, sufficiently clear rules are required to safeguard the rights to personal data protection and private life under Articles 7 and 8 of the Charter.

The EU legislator should accompany the requirement for hosting service providers to preserve content that has been removed or disabled as a result of a removal order with sufficiently specific safeguards. For this reason, the EU legislator should consider:

---

[56] ECtHR, *Roman Zakharov v. Russia [GC]*, No. 47143/06, 5 December 2015, para. 260; CJEU, *Digital Rights Ireland and Seitlinger and others [GC], Joined cases C-293/12 and C-594/12, 8 April 2014*, paras. 58, 65; CJEU, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others [GC], Joined cases C-203/15 and C-698/15,* 21 December 2016, paras. 111, 119.

[57] CJEU, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others [GC], Joined cases C-203/15 and C-698/15,* 21 December 2016, paras. 76-81.

[58] *Ibid*, para. 120.

[59] *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 105/54, 13 April 2006, pp 54-63.

[60] CJEU, *Digital Rights Ireland and Seitlinger and others [GC], Joined cases C-293/12 and C-594/12, 8 April 2014*, para. 62 and the operative part.

[61] ECtHR, *Roman Zakharov v. Russia [GC]*, No. 47143/06, 5 December 2015, paras. 231, 250, 253.

[62] *Ibid.*, para. 302.

- ***stating in Recital (23) that "Member States should lay down clear and precise rules indicating in what circumstances and under what conditions competent national authorities can access the preserved content and any related data. Access to such content and data must be subject to a prior review by a court or independent administrative body, except in cases of validly established urgency."***
- ***adding a sentence at the end of Article 7 (1) stating that "Except in cases of validly established urgency, access to terrorist content and related data for any of the purposes under point (b) shall be authorised only after a prior review by a court or other independent administrative authority according to national legislation."***
- ***adding a new second sentence in Article 7 (2) stating that "Related data preserved shall be erased after this period." The same requirement could be reflected in Recital (22).***

3 Adjusting the referrals' mechanism to avert unlawful interferences with fundamental rights

Article 5 of the proposal grants competent authorities of Member States or relevant EU bodies the possibility to refer content to hosting service providers for their expeditious "voluntary consideration". In response, the hosting service provider shall quickly ("as a matter of priority") assess the content identified by the referral against its own terms of service and decide whether such content should be removed or disabled. Hosting service providers shall provide feedback to the relevant authority, of the outcome and timing of any action taken as a result of the referral. This would bring the existing referral-based cooperation of Europol and Member States' law enforcement agencies with internet companies, designed to deal with online content that may contribute to radicalisation and extremism, under the ambit of the proposed Regulation. Although the consideration of referrals by hosting service providers is described in Article 5 (2) as "voluntary", failure to do so exposes them to penalties pursuant to Article 18 of the proposal.

The Chapter analyses the impact of the aforementioned provision on the freedom of expression and information under Article 11 of the Charter, due to the actual removal of content considered to be terrorist. It also looks at the impact on the freedom to conduct a business under Article 16 of the Charter, due to the requirement upon the hosting service providers to assess any content referred to them by the authorities against their terms of service, and take the appropriate action.

3.1 Strengthening Member States' obligation to protect fundamental rights online

According to the proposed Article 5 (4), the referral mechanism should be applied to content "considered terrorist content" by the competent authority. The Explanatory Memorandum confirms that the definition of 'terrorist content' in Article 2 (5) of the proposal evenly applies to removal orders, referrals and proactive measures. According to the proposed Article 4 on removal orders, in cases of any content falling under the ambit of the definition of 'terrorist content', the competent authorities would have at their disposal the mechanism of removal orders which requires the mandatory removal of or disabling of access to terrorist content. Relevant recitals and the Explanatory Memorandum do not provide an explanation as to the difference between the content justifying the competent national authority's use of a removal order, and other content, which is also considered terrorist but would require resorting to the use of a referral.

This opens a question of the criteria according to which the relevant competent national authority should decide on whether to order a removal or opt to delegate the responsibility to the hosting service provider. It also poses the question why a hosting service provider should be better placed to assess and possibly remove content which, presumably, has not warranted the issuing of a removal order by the competent authority. While it is entirely possible that online content can be considered illegal on other grounds (e.g. child pornography), removal of such content falls outside the subject matter of the current proposal and should not be pursued by measures aimed at combating terrorism. This lack of clarity could lead to the risk of improper use of the instrument of referrals, particularly in cases where the procedure at the national level for issuing them may be less stringent than that for issuing removal orders.

For these reasons, the introduction of referrals in the proposed manner into EU law, could in fact undermine rather than strengthen the legitimacy and effectiveness of the existing, functioning cooperation of Europol and Member States' law enforcement agencies with internet companies.

The concept of referrals also leads to the broader questions of transparency, effectiveness and accountability of the proposed measures. In the absence of any additional explicit safeguards, it is not clear what the accountability of public authorities would be in situations where they would initiate a removal of legitimate content via a referral. In this context, the Member States' positive obligation to prevent non-justifiable limitations of fundamental rights imposed by private entities needs to be underlined, especially if Member States themselves encourage such conduct. In this regard, there must be a clear distinction between Member States' duty to protect and hosting service providers' responsibility to respect fundamental rights.[63] According to the relevant guidelines of the Council of Europe, public authorities shall avoid any activity that exerts pressure on internet intermediaries through non-legal means.[64] The lack of legal clarity would be further compounded by the fact that hosting service providers are asked to assess the referred content solely against their own community standards. Terms of service or community standards often lack sufficient clarity and do not meet the requirement of 'legality' under international human rights law.[65] Furthermore, they do not reference human rights and related responsibilities.[66] In this context, the obligation under Article 10 of the proposal to establish complaint mechanisms for content providers whose content was removed or disabled as a result of a referral, cannot be considered a sufficient safeguard for potential fundamental rights infringements, as it does not – on its own – meet the requirements of an effective remedy required under Article 47 of the Charter.[67] Nor can it absolve the competent authorities of their responsibility.

Furthermore, receiving a referral from a competent authority could be understood as establishing actual knowledge about the presence of illegal content hosted by the online platform within the meaning of Article 14 of Directive 2000/31/EC (E-Commerce Directive),[68] hence leading to the hosting service providers liability. The risk of losing the protection under the E-Commerce Directive may lead hosting service providers to take steps to avoid the danger of liability and the imposition of high fines, including under Article 18 of the proposed Regulation for not meeting their specific obligations under the referral mechanism, creating an incentive for the over-removal of content, including legitimate content. This would amount to a "chilling effect" and

---

63 European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*, p. 5.

64 Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, *Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities*, para. 1.1.1.

65 *Letter of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism concerning Facebook's overly broad definition of terrorism*, OL OTH 46/2018, 24 July 2018.

66 United Nations (2018), *Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, OL OTH 71/2018, p. 7-8.

67 FRA (2017), *Improving access to remedy in the area of business and human rights at the EU level*, 10 April 2017.

68 *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 July 2000, pp. 1-16.

increase the likelihood of unjustified interferences with the right to freedom of expression and information, as protected by Article 11 of the Charter.

FRA Opinion 9

The proposal does not sufficiently justify the necessity of introducing the mechanism of referrals under Article 5 through which competent authorities could instruct hosting service providers to assess specific content against their terms of service and community standards, and potentially remove it. If they are introduced alongside other measures in the proposal, particularly mandatory removal orders, without clearly distinguishing the circumstances in which they should be used, it carries the risk of expanding the scope of what is understood as terrorist content, blurring the responsibility for assessing the online content and undermining the legal certainty regarding liability of hosting service providers. These implications, together with the proposed system of penalties, could lead to a chilling effect on the freedom of expression and information protected under Article 11 of the Charter.

The EU legislator should introduce clear rules to distinguish between content that would justify issuing a removal order, and other terrorist content which would require resorting to a referral.

Furthermore, the EU legislator should consider omitting the reference to Article 5 and referrals in Article 18 (1) (c) requiring Member States to introduce penalties upon hosting service providers.

Finally, the EU legislator should consider including a reference to the positive obligation of the Member States to secure the effective exercise of fundamental rights and prevent fundamental rights violations in a relevant recital.

4 Establishing proactive measures that respect the fundamental rights of users and hosting service providers

Article 6 of the proposed Regulation allows hosting service providers to adopt proactive measures to fight against the dissemination of terrorist content, including by automated means. According to the proposed Article 6 (1), they shall take the initiative to adopt such measures, in which case the proposal requires that the measures are proportionate and respect fundamental rights. Pursuant to Article 6 (2) of the proposal, hosting service providers are also required to report on proactive measures taken in response to a removal order. This is to prevent the re-upload of the removed content and, more generally, to detect, identify and expeditiously remove or disable access to terrorist content. Where the competent authority considers these to be insufficient, it may request or impose additional proactive measures. Proposed Article 6 (5) provides that a hosting service provider may request the competent authority to review and revoke its request for proactive measures or its decision imposing these. The draft Regulation does not, however, provide clarity whether the affected hosting service providers would be able to request an external independent and impartial review of the competent authority's decision.

This Chapter covers the issue of responsibility for possible fundamental rights violations by actions of private actors, particularly as regards the freedom of expression and information under Article 11 of the Charter. It also touches on the rights to private life (Article 7) and the protection of personal data (Article 8). In addition, it looks at the hosting service providers' right to an effective remedy (Article 47 of the Charter) given the implications of the obligation to apply proactive measures on the freedom of expression as well as the freedom to conduct a business under Article 16 of the Charter.

4.1 Safeguarding due diligence

Article 3 of the proposal requires that when taking actions to prevent the dissemination of terrorist content, hosting service providers shall act in a diligent, proportionate and non-discriminatory manner and with due regard to the fundamental rights of users. It underlines the "fundamental importance of the freedom of expression and information in an open and democratic society." Proposed Recital (17) adds that hosting service providers should act with due diligence to avoid any unintended and erroneous decision leading to the removal of content that is not terrorist content. This means that unlike in case of removal orders under Article 4, the hosting service providers themselves should assess the content and then ensure that it is removed from their platforms. At the same time, they also bear the responsibility for interferences with, and possible violations of, fundamental rights when they remove non-terrorist content.

Yet, it is for the state and not a private party to secure the rights and freedoms of everyone within its jurisdiction. In order to secure the effective exercise of the freedom of expression and information under Article 11 of the Charter requires Member States to adopt positive measures to protect the human rights of individuals online and offline, striking a fair balance between the freedom of expression and

information, and the private entities' freedom to conduct a business, as guaranteed by Article 16 of the Charter.[69]

EU Member States' positive obligation would require that the public authorities must ensure that fundamental rights impact assessments are being conducted by host service providers on regular basis. They should equally provide guidelines to online platforms on how to bring their terms of service or community standards in line with fundamental rights principles. In this context, a reference can also be made to the Council of Europe Guide to Human Rights for Internet Users which stipulates that states have an obligation to ensure that any general terms and conditions of private sector entities that are not in accordance with international human rights standards, must be held null and void in domestic legal systems of Council of Europe Member States.[70]

The monitoring requirement proposed in Article 6 can in practice be performed only by automated detection tools and filtering systems. Indeed, under proposed Article 6 (2), proactive measures employed by hosting service providers may include automated tools. Recital (18) of the proposal specifically refers to the use of reliable technical tools to identify new terrorist content. However, the character of online communication is deeply context-dependent and intersubjective. In this context, it is remarkable that Article 9 (2) of the proposal only requires hosting service providers to implement human oversight and verifications "where appropriate", rather than employing human methods by default and in all cases for assessing whether or not specific content should be removed.

In order to be effective, such tools have to be applied to all user-generated content hosted by online platforms, likely already at the point of upload. This would result in general monitoring of content which would not be compatible with the online users' right to freedom of expression pursuant to Article 11 of the Charter. It would also carry risks for the rights to private life and the protection of personal data of other persons (Articles 7 and 8 of the Charter), including those who are not users of the platforms but whose information might be processed as part of the screening of the users' content.[71] In addition, this would not be compatible with the relevant recommendations of the Council of Europe in this field.[72]

Imposing such a general monitoring obligation is also prohibited by Article 15 of the E-Commerce Directive. Recital (19) of the proposal advocates for derogations from Article 15 due to a "particularly grave risk imposed by dissemination of terrorist content online." The E-Commerce Directive, however, does not allow for any exemptions from this prohibition. In *Sabam v. Netlog*, the CJEU concluded that a filtering system, which targets a specific type of content while indiscriminately monitoring all information shared by platform users for unlimited period of time, amounts to such a prohibited general monitoring obligation.[73] Although the case concerns copyright infringements, the applied filtering technique remains the same, regardless of the different types of targeted content.

---

69 ECtHR, *VgT Verein Gegen Tierfabriken v. Switzerland*, No. 24699/94, 28 June 2001, para. 45. See also ECtHR, *Delfi AS v. Estonia [GC]*, No. 64569/09 2015, 16 June 2015, para. 138.

70 Council of Europe (2014), *Guide to human rights for Internet users*, contained in an Appendix to Recommendation of the Council of Europe's Council of Ministers CM/Rec(2014)6, 16 April 2014, para. 5.5.

71 ECtHR, *Delfi AS v. Estonia*, No. 64569/09, 16 June 2015, para. 138.

72 See for instance Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, *Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities*, para. 1.3.5.

73 CJEU, *SABAM v. Netlog NV*, C-360/10, 16 February 2012.

The requirement of Article 6 (2) (a) to prevent the re-upload of previously removed content is also open to interpretation, as the proposal does not clarify to what extent this limits the filtering to identical copies only, and which technical solutions will need to be involved for different types of content. Preventing the re-appearance of previously identified terrorist content will require comparing all newly uploaded content to a database gathering content already recognised as terrorist. Due to the quantity of user-generated content, such systems will realistically be run by algorithms which will require access to high quality data on which they can be trained.

The Impact Assessment accompanying the proposal acknowledges a range of fundamental rights concerns related to the reliance on proactive measures to prevent the dissemination of online terrorist content. This includes the risk of possible biases, inherent errors and discrimination that can lead to erroneous decisions in algorithmic decision-making.[74] It states that the impact on the freedom of expression and information would in such circumstances "depend largely on the accuracy of such tools and how well calibrated they are in terms of avoiding false positives."[75] In this regard, it recognises the immaturity of language processing systems for identifying illegal hate speech and other type of harmful speech, as well as the frequent misidentification of visual content.[76] The Agency has elaborated on these issues in its May 2018 Focus Paper. According to the findings, the use of algorithms in decision-making can bring welcome benefits, such as consistency and objectivity. However, it also entails serious risks, as it can result in, or exacerbate, discrimination.[77]

Finally, the formulation of Article 6 (2) implies the obligation of a hosting service provider to adopt proactive measures in all cases where it has been an addressee of a removal order. This does not seem to reflect the different level of exposure to terrorist content that such providers might be facing, and may lead to disproportionate effect on the freedom to conduct a business as well as to a proliferation of proactive measures impacting on the freedom of expression and information. Therefore, the proportionality of these measures would be enhanced if they were narrowly targeted to those hosting service providers that have been used, demonstrably and to a significant extent, for dissemination of illegal terrorist content, i.e. been subject to a considerable number of justified removal orders.[78]

FRA Opinion 10

By introducing in Article 6 a broad obligation upon hosting service providers to apply proactive measures to assess and potentially remove content and at the same time making them fully responsible for potential interferences with fundamental rights, the proposal raises issues of compatibility with the positive obligations of the state under the Charter. Obligations under the proposed Article 6 may lead to general monitoring of content, which would not be compatible with online users' right to freedom of expression and information pursuant to Article 11 of the Charter. They also carry risks for the rights to private life and protection of personal data of other persons under

---

74 European Commission (2018), *Commission Staff Working Document - Impact Assessment Accompanying the Document Proposal for a regulation of the European parliament and of the Council on preventing the dissemination of terrorist content online*, SWD(2018) 408 final, Brussels, 12 September 2018, p. 15.

75 *Ibid.*, p. 105.

76 *Ibid.*, pp. 13, 40-41.

77 FRA (2018), Focus Paper *#BigData: Discrimination in data-supported decision making*, May 2018.

78 Blanco, L., Jeppesen, J.-H., *Terrorist Content Regulation: MEPs Should Support IMCO and CULT Committees Proposals*, Center for Democracy and Technology, 25 January 2019.

Articles 7 and 8 of the Charter. The impact of enhanced use of automated means and artificial intelligence software, encouraged by the proposal, would significantly impact on the rights of freedom of expression and information and non-discriminatory treatment of online users, also due to the limited reliability of such tools.

The EU legislator should consider deleting Article 6 (1) obliging hosting service providers to apply proactive measures. A relevant recital should instead refer to the positive obligation of the Member States to secure the effective exercise of fundamental rights and prevent fundamental rights violations, including by providing necessary guidance to hosting services providers to ensure that their content restricting polices set out in the general terms and conditions pay due regard to the relevant human rights standards; and underline that the effectiveness of software used to detect terrorist content should be adequately tested, especially from a fundamental rights perspective.

The EU legislator should clarify in Article 6 (2) that the provision aims at preventing the re-appearing of content identical to that previously identified as terrorist, and removed on the basis of a removal order. Furthermore, it should ensure by amending Recital (19) that the proposal does not permit any conflict with EU law, namely by allowing for a derogation from the prohibition of general monitoring obligation, as enshrined in Article 15 of the E-Commerce Directive.

At the same time, the EU legislator should also clarify in Recital (18) that Article 6 (2) should not be interpreted as requiring any hosting service provider to whom a removal order had been addressed to introduce proactive measures, and that the competent authority referred to in Article 17 (1) (c) should take into account the level of exposure of the host service providers to terrorist content.

4.2 Ensuring the right to an effective remedy for hosting service providers against decisions imposing additional proactive measures

According to Article 47 of the Charter, it is for EU Member States to establish a system of legal remedies and procedures that ensure respect for rights under EU law.[79] The right of access to a court is not absolute and can be limited, for example by imposing reasonable time limits that promote the proper administration of justice.[80] Access to a court can well depend on prior exhaustion of available remedies before competent administrative authorities.[81] However, such a requirement should not disproportionately affect the right to bring an action before a court. It should not lead to substantial delay, nor involve excessive costs, and should include the suspension of limitation periods (prescription).[82] Legislation not providing any possibility for an individual to pursue legal remedies does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.[83]

Hosting service providers are obliged to take proactive measures, following a request or a decision by the competent authority. Recital (8) of the proposed Regulation refers

---

79 CJEU, *Unibet (London) Ltd and Unibet (International) Ltd v. Justitiekanslern*, C-432/05, 13 March 2007, paras. 37-42.

80 FRA (2016), *Handbook on European law relating to access to justice*, Luxembourg, Publications Office, p. 28.

81 CJEU, *Peter Puškár v. Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy*, Case C-73/16, 27 September 2017, para. 70.

82 *Ibid.*, para. 71.

83 CJEU, *Maximillian Schrems v. Data Protection Commissioner,* C-362/14, 6 October 2015, para. 95.

to the right of each natural or legal person "to an effective judicial remedy before the competent national court against any of the measures taken pursuant to this Regulation". Nevertheless, it only specifically mentions the situation of hosting service providers and content providers to effectively contest the removal orders before the court of the Member State whose authorities issued the removal order. Article 6 which regulates the mechanism of proactive measures, refers to a review by the same competent authority. In other words, the proposal does not require involvement of a court in review of decisions taken pursuant to Article 6 (4), nor does it take into account the complexities of cross-border scenarios. This is despite the fact that proactive measures, especially those which are explicitly imposed by a decision, interfere with the rights of both the hosting service provider and content providers. In addition, imposing proactive measures involves costs and other organisational burdens for hosting service providers, hereby interfering with their freedom to conduct a business, as guaranteed under Article 16 of the Charter.

FRA Opinion 11

The proposal establishes in Article 6 (4) that the competent authority can issue a decision requiring hosting service providers to take specific additional proactive measures on a mandatory basis. At the same time, it only provides for a review by the same competent authority, without requiring that such review should be conducted by a court, contrary to the minimum requirements for an effective remedy under Article 47 of the Charter.

The EU legislator should ensure the right to an effective remedy for hosting service providers against the mandatory imposition of additional proactive measures by amending Article 6 (5) to state that decisions taken pursuant to Article 6 (4) shall be subject to review by a court.

TK-01-19-164-EN-N

Publications Office

ISBN: 978-92-9474-244-5
doi: 10.2811/818523

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

FRA – European Union Agency for Fundamental Rights

Schwarzenbergplatz 11 ▪ 1040 Vienna ▪ Austria ▪
Tel +43 158030-0 ▪ Fax +43 158030-699
fra.europa.eu ▪ info@fra.europa.eu ▪ facebook.com/fundamentalrights
▪ linkedin.com/company/eu-fundamental-rights-agency ▪
twitter.com/EURightsAgency