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

REFERENCE:
OL OTH 71/2018

7 December 2018

Excellency,

We have the honour to address you in our capacities as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; Special Rapporteur on the right to privacy and Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, pursuant to Human Rights Council resolutions 34/18, 37/2 and 31/3.

I. INTRODUCTION

On 12 September 2018, the Commission of the European Union launched a Proposal for a Regulation on preventing the dissemination of terrorist content online to complement Directive 2017/541 on combating terrorism.[1] The proposal also complements the Commission's Communication on tackling illegal content online, towards enhanced responsibility of online platforms[2] and Commission Recommendation on measures to effectively tackle illegal content online[3], setting up a voluntary framework of action for Internet intermediaries. The initiative comes on the heels of the European Parliament calling on the Commission to present proposals "to strengthen measures to tackle illegal and harmful content"[4] and similar calls made by a number of Member States.[5] The declared aim of the Proposal is to ensure that Internet platforms offering their services in the European Union are "subject to clear rules to prevent their services from being misused to disseminate terrorist content".[6] In this respect, the draft Regulation provides a definition of terrorist content and sets up a framework for addressing such content, including by outlining the responsibility of Internet intermediaries in this regard. The Explanatory Memorandum to the Proposal also stresses the intention to introduce "a number of necessary safeguards to ensure full respect for fundamental rights such as

1 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.

2 European Commission, 'Communication on tackling illegal content online, towards enhanced responsibility of online platforms' (28 September 2017).

3 Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final).

4 European Parliament resolution of 15 June 2017 on online platforms and the digital single market (2016/2276(INI)).

5 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Explanatory memorandum, p. 2.

6 European Commission, State of the Union 2018: Commission proposes new rules to get terrorist content off the web, Strasbourg, 12 September 2018, available at http://europa.eu/rapid/press-release_IP-18-5561_en.htm.

freedom of expression and information in a democratic society". Given the overarching function of our mandates to advance the protection and promotion of human rights and acknowledging that the Proposal has significant human rights implications, we convey our views to support the work of relevant European Union organs in advancing full respect for human rights.

Recognizing the challenging regulatory context and the laudable goal of using legal tools to prevent misuse of Internet platforms in the context of terrorism, we raise these matters of general concern. In particular, we wish to express our views regarding the overly broad definition of terrorist content in the Proposal that may encompass legitimate expression protected under international human rights law. We note with serious concern what we believe to be insufficient consideration given to human rights protections in the context of to the proposed rules governing content moderation policies. We recall in this respect that the mechanisms set up in Articles 4-6 may lead to infringements to the right to access to information, freedom of opinion, expression, and association, and impact interlinked political and public interest processes. We are further troubled by the lack of attention to human rights responsibilities incumbent on business enterprises in line with the United Nations Guiding Principles on Business and Human Rights. We recommend that the Proposal be amended with due consideration to the human rights concerns outlined below. This communication is very specific in offering views which may assist the European Union in taking forward a fully human rights compliant approach in this regulatory context.

II. CONCERNS REGARDING THE PROPOSAL FOR A REGULATION ON PREVENTING THE DISSEMINATION OF TERRORIST CONTENT ONLINE UNDER INTERNATIONAL HUMAN RIGHTS LAW

1. Definition of terrorist content

Article 2(5) of the proposal defines 'terrorist content' as:

(a) inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;

(b) encouraging the contribution to terrorist offences;

(c) promoting the 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;

(d) instructing on methods or techniques for the purpose of committing terrorist offences.

The definition builds on Article 5 of the Directive on combating terrorism delineating the scope of the crime of 'public provocation to commit a terrorist offence' as the "distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission" of a terrorist offence as defined in Article 3(1) of the Directive where such conduct, "directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed".

The Special Rapporteurs note that Article 5 of the Directive sets out the crime of public provocation to commit a terrorist offence in broad terms. It does so by encompassing indirect advocacy and the insufficiently defined 'glorification' of terrorist acts and setting a low threshold by only requiring that the conduct 'causes a danger' that offences 'may be committed', as opposed to conduct that creates an actual risk or an imminent danger of harm. In the Special Rapporteurs' view, this threshold lacks the precision required by the principle of legality. This shortcoming may also lead to the imposition of sanctions that are disproportionate to the severity of and social harm caused by the proscribed conduct. The Directive has for this reason been subject to criticism by human rights organizations.[7]

Article 2(5) of the Proposal however goes significantly further by omitting the element of intent altogether. This is a very serious and disappointing regulatory development. The Proposal also broadens the scope of expression that would be considered "terrorist" by including encouraging the contribution, participation or support to terrorism or a terrorist group. The definition as it stands could encompass legitimate forms of expression, such as reporting conducted by journalists and human rights organizations on the activities of terrorist groups and on counter-terrorism measures taken by authorities, in violation of the right to freedom of expression as protected under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), Article 10 of the European Convention of Human Rights (ECHR), and Article 11 of the Charter of Fundamental Rights of the European Union (the EU Charter).

The Special Rapporteurs wish to emphasize that the right to freedom of expression extends '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 that pluralism, tolerance and broadmindedness without which there is no "democratic society"'.[8] Moreover, as the right to access to information extends to all types of information, States "bear the burden of justifying any withholding of information as an exception to that right".[9]

United Nations human rights mechanisms have stressed that freedom of expression is a prerequisite for the effective promotion and protection of a broad range of human rights, including rights that cannot be lawfully limited such as freedom of opinion. Therefore, as a matter of principle, limitations on freedom of expression must remain the exception and should be applied strictly so as to "not put in jeopardy the right itself".[10]

---

7 See, for example, Amnesty International, the European Network Against Racism (ENAR), European Digital Rights (EDRi), the Fundamental Rights European Experts (FREE) Group, Human Rights Watch, the International Commission of Jurists (ICJ), and the Open Society Foundations (OSF), 'EU Counterterrorism Directive Seriously Flawed', 30 November 2016, available at https://www.hrw.org/news/2016/11/30/eu-counterterrorism-directive-seriously-flawed.

8 *Handyside v. the United Kingdom*, no. 5493/72, 7 December 1976, § 49.

9 A/70/361, para. 8.

10 UN Human Rights Committee, General Comment No. 34, Article 19: Freedoms of opinion and expression, UN Doc. CCPR/C/GC/34, para. 21.

Such limitations must have a clear legal basis in domestic law, "sufficiently accessible and foreseeable as to its effects, that is, formulated with sufficient precision to enable the individual to regulate his conduct" and to enable those affected by it "to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[11] The requirement of legality also serves to define the scope of legal discretion conferred on implementing authorities in order to provide adequate protection against arbitrary implementation.[12]

Restrictions on the right to freedom of expression must pursue a legitimate aim and be necessary in a democratic society. This requirement also implies an assessment of the proportionality of the relevant measures, with the aim of ensuring that restrictions "target a specific objective and do not unduly intrude upon the rights of targeted persons".[13] The restrictions must be "the least intrusive instrument among those which might achieve their protective function and proportionate to the interest to be protected."[14] Finally, permissible restrictions regarding online content are the same as those applicable offline.[15]

While human rights covenants recognize national security and public order as legitimate aims for restricting freedom of expression, the Human Rights Council has stressed "the need to ensure that invocation of national security, including counter-terrorism, is not used unjustifiably or arbitrarily to restrict the right to freedom of opinion and expression".[16] In this regard, the Special Rapporteur on freedom of expression has concluded that States should "demonstrate the risk that specific expression poses to a definite interest in national security or public order, that the measure chosen complies with necessity and proportionality and is the least restrictive means to protect the interest, and that any restriction is subject to independent oversight."[17]

The strict adherence to the above set out test is the more crucial when States decide to criminalize certain forms of expression. In this respect, the Special Rapporteurs wish to highlight that the mandate of the Special Rapporteur on counter-terrorism and human rights has formulated definitions of terrorism and incitement to terrorism. These definitions reflect best practice in countering terrorism, pursuant to an analysis undertaken on the basis of consultations and various forms of interaction with multiple stakeholders, including Governments.[18]

In this respect, we draw your attention to the model definition based on best practice for the offense of terrorist incitement:

---

[11] *Sunday Times v. United Kingdom (no. 1)*, no. 6538/74, 26 April 1979, § 49; U.N. Doc. CCPR/C/GC/34, para. 25.

[12] *Malone v. United Kingdom*, no. 8691/79, Series A no. 82, 2 August 1984, § 68.

[13] A/HRC/29/32, para 35; UN Human Rights Committee, General Comment No. 27, Freedom of movement (Art. 12), UN Doc. CCPR/C/21/Rev.1/Add.9 (2 November 1999).

[14] UN Human Rights Committee, General Comment No. 34, Article 19: Freedoms of opinion and expression, UN Doc. CCPR/C/GC/34, para. 34; A/HRC/32/38, para. 7.

[15] A/HRC/17/27, para. 69; A/HRC/RES/38/7, para. 1.

[16] A/HRC/RES/7/36.

[17] A/71/373, para. 18.

[18] A/HRC/16/51, Practices 7 and 8.

> It is an offence to intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed.[19]

We urge the European Union to amend Article 2(5) of the proposal by bringing it in line with the model definition. We further highlight the lack of clarity as to whether content covered by Article 2(5) amounts to criminal conduct. In this regard, we flag that the definition appears to go beyond the scope of terrorist offences set out in the Directive on combating terrorism. Finally, as incitement and related offences such as advocacy and glorification of terrorism constitute inchoate crimes, we urge that due consideration be given to the required threshold of harm needed to justify the criminalization of expression. In line with the recommendations of human rights mechanisms and the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (Rabat Plan of Action),[20] the threshold would require the reasonable probability that the expression in question would succeed in inciting a terrorist act, thus establishing a degree of causal link or actual risk of the proscribed result occurring.[21]

The Special Rapporteurs emphasize the importance of restricting counter-terrorism measures to conduct that is truly terrorist in nature. In this vein, all counterterrorism laws "must be limited to the countering of offences within the scope of, and as defined in, the international conventions and protocols relating to terrorism, or the countering of associated conduct called for within resolutions of the Security Council, when combined with the intention and purpose elements identified in Security Council resolution 1566 (2001)".[22] Conversely, "[c]rimes not having the quality of terrorism (…), regardless of how serious, should not be the subject of counter-terrorist legislation".[23]

The Special Rapporteurs, however, note that content that cannot genuinely be characterized as terrorist may nonetheless be unlawful. In particular, such content may amount to advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. Such content should be addressed in line with Articles 20 and 19(3) of the International Covenant on Civil and Political Rights. In conducting relevant assessments, the Special Rapporteurs recommend that the European Union be guided by the standards spelled out in the Rabat Plan of Action, in particular the six-part threshold test set out therein. This test considers the following elements when

---

19 A/HRC/16/51, Practice 8.

20 A/HRC/22/17/Add.4

21 Rabat Plan of Action, UN Doc. A/HRC/22/17/Add.4, para. 29; *Erbakan v. Turkey*, no. 59405/00, 6 July 2006, § 68. See also, Toby Mendel, Study on International Standards Relating to Incitement to Genocide or Racial Hatred, a study for the UN Special Advisor on the prevention of Genocide, April 2006, p. 50. Note that the former Special Rapporteur on counter-terrorism and human rights also stressed that the crime of incitement required an "an objective danger of a terrorist offence being committed". A/HRC/16/51, Practice 8, para. 30.

22 E/CN.4/2006/98, para. 39.

23 *Ibid.* para. 47.

assessing speech that may amount to advocacy of hatred: (1) context; (2) speaker; (3) intent; (4) content and form; (5) extent of the speech act; and (6) likelihood, including imminence.[24]

Finally, the Special Rapporteurs reiterate that "expression that does not give rise to criminal, civil or administrative sanctions, but still raises concern in terms of tolerance, civility and respect for the rights of others" may only be restricted in line with Article 19 ICCPR, Article 10 ECHR and Article 11 of the EU Charter.[25]

2. Removal orders under Article 4 of the Proposal

Article 4 of the Proposal provides for the obligation of hosting service providers to remove terrorist content or disable access to it within one hour from receipt of a removal order issued by a competent authority. The Special Rapporteurs note their exceptional concern at the short timeline for complying with orders provided under the proposal. We highlight the likely negative implications this timeline presents to the practical realization of protection for freedom of expression and interlinked rights in real time. The accelerated timeline does not allow Internet platforms sufficient time to examine the request in any detail, required to comply with the sub-contracted human rights responsibilities that fall to them by virtue of State mandates on takedown. This deficiency is compounded by the fact that even if the respective company or the content provider decide to request a detailed statement of reasons,[26] this does not suspend the execution of the order, nor does the filing of an appeal. Both the extremely short timeframe and the threat of penalties are likely to incentivize platforms to err on the side of caution and remove content that is legitimate or lawful. This may have profound effects on the experience of rights violations and undermine the potential for meaningful remedies to be quickly activated.

Furthermore, the Proposal does not specify whether the competent authorities designated by Member States would benefit from any level of institutional and substantive independence from the executive, or that they should adhere to standards of impartiality and due process. The Special Rapporteur on freedom of expression has urged States to ensure that content removals are undertaken "pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy".[27] We underscore that the Proposal makes no reference to any requirement that those deciding on removal orders would have the requisite expertise in the area of human rights and fundamental freedoms that would allow for a meaningful assessment of the human rights implications of actions taken. This creates substantial human rights compliance concerns.

---

[24] Rabat Plan of Action, UN Doc. A/HRC/22/17/Add.4, para. 29.

[25] *Ibid.*, para. 20.

[26] The Special Rapporteurs note that no timeline is included within which the competent authority needs to provide a detailed statement of reasons.

[27] A/HRC/38/35, para. 66.

3. Referrals under Article 5 of the Proposal

Article 5 of the Proposal provides for the possibility for competent authorities, at Member State or Union level, to send referrals regarding terrorist content to hosting service providers for their voluntary consideration.

Article 5 specifies that referrals shall outline the reason why the content in question is to be considered "terrorist content". However, it does not explicitly clarify whether the competent authority is to use the definition of terrorist content codified in domestic and EU law or may rely on the definitions used by hosting service providers, which may be considerably broader and inconsistent with standards set up under international law.[28] The Special Rapporteurs emphasize that referrals in relation to terrorist content should always be based on grounds foreseen in domestic law, in line with State obligations to ensure that restrictions on freedom of expression have a legal basis in domestic law, and urge that this requirement be explicitly reflected in the text of the Regulation. Doing otherwise would risk removing the referral process from the confines set up by the rule of law and may result in undermining safeguards against unlawful or arbitrary interference, including the right to access to an effective remedy. It may further enable authorities to request private actors to remove or disable content that said authorities could not restrict in line with their obligations under domestic and international law.

The risks described above are compounded as hosting service providers are to assess referrals against their terms of service or community standards. We note that such terms of service or community standards do not reference human rights and related responsibilities, thereby creating the possibility of an 'escape route' from human rights oversight.

The Special Rapporteurs note that terms of service and community standards frequently impose limitations beyond what States could do in compliance with their obligations under international human rights law.[29] They are commonly drafted in terms that lack sufficient clarity and fail to provide adequate guidance on the circumstances under which content may be blocked, removed or restricted, or access to a service may be restricted or terminated, thereby falling short of the legality requirement under international human rights law. These shortcomings become particularly problematic when such hosting service providers play a role in areas traditionally ascribed to States, such as by exercising quasi-regulative, quasi-enforcement and quasi-adjudicative functions in the context of the fight against terrorism. We underscore the obligations of States to ensure that such sub-contraction of State enforcement obligations occur in a human rights-compliant manner. The Human Rights Committee has observed that, under Article 2(1) of the ICCPR, the obligation to "ensure" rights under the Covenant implies a

---

[28] See, for example, Letter of the Special Rapporteur on the promotion and protection of human rights and fundamental freedom while countering terrorism concerning Facebook's overly broad definition of terrorism and the apparent lack of a comprehensive human rights-based approach to the policies governing access to and use of its platform, OL OTH 46/2018, available at https://www.ohchr.org/Documents/Issues/Terrorism/OL_OTH_46_2018.pdf.

[29] In this sense see, for example A/HRC/38/35, in particular the relevant standards set out in paras. 44-48.

duty to "take appropriate measures or exercise due diligence to prevent, punish, investigate or redress the harm" caused by private persons or entities.[30] We take the view that this duty to protect individuals from "acts committed by private persons or entities" is heightened when States engage businesses, including technology platforms, to advance their enforcement preferences.

Under the Proposal as drafted, the responsibility for removing content pursuant to a referral, at least towards the content provider, stays with the platform. In this respect, the Proposal states that platforms are under the obligation to set up a complaint mechanism that content providers can use to challenge removals of content. Complaint mechanisms set up by companies however do not offer the same guarantees and safeguards as processes before public authorities, be they administrative or judicial, and may fall short of providing redress for undue interferences with human rights and fundamental freedoms, as required under international human rights law. Such a mechanism will not relieve States of their treaty-based human rights obligation, and in our view, the failure to protect will fall within the ambit of State responsibility.[31]

At the same time, platforms are required to assess referrals as a matter of priority and inform the authorities of the outcome expeditiously. Failure to comply with these requirements could lead to the imposition of proactive measures or even penalties. This setting is, in our view, likely to lead to a tendency to over-regulate expression on part of hosting service providers in case of doubt or shortage of resources. This is all the more so considering the uneven consequences resulting from unwarranted removals, on the one hand, and not addressing referred content in a way that will satisfy the competent authority, on the other. Moreover, as removals based on violations of terms of service are in principle effective globally (as opposed to content removals based on orders which are commonly restricted to the jurisdiction having issued the order), the likely human rights violations in case of undue removals are even further-reaching.

The approach sanctioned in Article 5 creates the risk that governments expand their possibilities to have content blocked, filtered, or removed beyond what is provided for under national law and what would be permissible under international human rights law. [32] Even if governments only request restrictions that they deem to be in accordance with the law, the referral process may result in undermining the regular safeguards that protect against excessive interference, including the right to an effective remedy. Having in mind that such referrals may be the result of non-transparent and unaccountable decision-making processes, with limited options for redress, potentially in violation of Article 2(3) ICCPR and Article 13 ECHR, the elevated risk of arbitrariness and abuse it presents is evident.

---

[30] General Comment No. 31 [80], The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add. 1326 May 2004, para. 8.

[31] See, Responsibility of States for Internationally Wrongful Acts, *Official Records of the General Assembly, Fifty-sixth Session, Supplement No. 10* (A/56/10), Art. 5.

[32] A/HRC/38/35, para. 19.

4. Proactive measures by hosting service providers under Article 6 of the Proposal

Article 6 of the proposed Regulation addresses proactive measures that hosting service providers may take at their own initiative or at the direction of a competent authority. In accordance with the Proposal, all Internet platforms that have received removal orders under Article 4 will have to report on such proactive measures within three months after the receipt of the order and thereafter at least on an annual basis. The proactive measures required in this context include preventing the re-upload of content that has been removed or disabled and "detecting, identifying and expeditiously removing or disabling access to terrorist content". The Proposal requests the use of automated tools in this regard. In case proactive measures are imposed by a competent authority, the affected hosting service providers may request the authority to review its decision. It is however unclear whether an independent external review of such decisions is possible. We view independent review as an essential aspect of ensuring a right to an effective remedy as guaranteed under the European Convention and the ICCPR.

The proactive measures outlined in Article 6 may amount to a general obligation to monitor content in contravention of Article 15 of the e-Commerce Directive[33] and would be in principle susceptible to lead to the loss of protection against liability for third-party content established under Article 14 of the same. They would also be incompatible with relevant recommendations by the Council of Europe Committee of Ministers.[34] While the Explanatory Memorandum to the Proposal and the Recitals state that "any measures taken by the hosting service provider in compliance with this Regulation, including any proactive measures, should not in themselves lead to that service provider losing the benefit of the liability exemption provided for, under certain conditions, in Article 14 of the E-Commerce Directive",[35] such guarantees are not repeated in the substantive provisions of the proposed Regulation.

The same observations are valid also with respect to the imposition of a general monitoring obligation. [36] However, both the Explanatory Memorandum and Recital 19 note that due to the "particularly grave risks associated with the dissemination of terrorist content", the "decisions adopted by the competent authorities on the basis of this Regulation could derogate from the approach established in Article 15(1) [of the e-Commerce Directive]". It also simultaneously notes that the competent authorities should strike a "fair balance between public security needs and the affected interests and fundamental rights including in particular the freedom of expression and information, freedom to conduct a business, protection of personal data and privacy". Again, these statements are not reflected in the substantive provisions of the draft Regulation.

---

[33] 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.

[34] **Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities. Appendix to** Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, 7 March 2018, para. 1.3.5.

[35] Proposal for a Regulation on preventing the dissemination of terrorist content online, Explanatory Memorandum, section 1.2.; Recital 5.

[36] Proposal for a Regulation on preventing the dissemination of terrorist content online, Explanatory Memorandum, section 1.2; Recitals 12, 16, 19.

Due to the lack of binding force attributed to recitals, such omissions may lead to legal uncertainty, impacting both businesses and individuals, and potentially undermining the protection of human rights.

The Special Rapporteurs are also concerned that a general monitoring obligation will lead to the monitoring and filtering of user-generated content at the point of upload. This form of restriction would enable the blocking of content without any form of due process even before it is published, reversing the well-established presumption that States, not individuals, bear the burden of justifying restrictions on freedom of expression.[37]

The Special Rapporteurs also note that the use of automated tools for content regulation, as required under the draft Regulation, comes with serious limitations and aggravates the risk of pre-publication censorship. [38] Algorithms frequently have an inadequate understanding of context and many available tools, such as natural language processing algorithms, do not have the same reliability rate across different contexts.[39] They have, at times, also been shown susceptible to amplifying existing biases.[40] Moreover, considering the volume of user content that many hosting service providers are confronted with, even the use of algorithms with a very high accuracy rate potentially results in hundreds of thousands of wrong decisions leading to screening that is over- or under-inclusive. The Special Rapporteurs note that Article 9 of the Proposal requests Internet platforms making use of automated tools to provide "effective and appropriate" safeguards to ensure that decisions taken pursuant to the Regulation are "accurate and well-founded". They however wish to highlight that ensuring accurate and well-founded decision-making involving the use of automated tools requires a human rights-based approach to be at the centre of the design, deployment, and implementation of artificial intelligence systems.[41] They further contend that such systems must be subject to human rights impact assessments, periodic independent audits, safeguards ensuring adequate user notice and consent, and robust oversight, including human oversight, of their functioning and use.[42]

5. Human rights responsibilities of hosting service providers

International organizations and governments have consistently called for enhanced cooperation between the public and private sectors to aid efforts to counter terrorism and violent extremism, "while respecting human rights and fundamental freedoms and complying with international law and the purposes and principles of the

---

37 The Special Rapporteur on freedom of expression raised similar concerns in the context of the EU draft directive on copyright in the digital single market: see OL OTH 41/2018.

38 For a detailed analysis of the human rights implications of artificial intelligence, see the latest report of the Special Rapporteur on freedom of expression, submitted to the 73rd session of the General Assembly, UN Doc. A/73/348, available at http://undocs.org/A/73/348.

39 A/73/348, para. 15.

40 *Id.*, paras. 36 – 38.

41 A/73/348, paras. 47 – 60.

42 A/73/348, paras. 62ff.

Charter".[43] The Special Rapporteurs recognize that successful tackling of the use of internet platforms for terrorist purposes requires meaningful cooperation between public authorities and relevant companies. They further note the role and influence of such companies in enabling and facilitating communication between a wide variety of stakeholders and, as a consequence, on the public's access to seek, receive and impart information.

Against this background, the Special Rapporteurs wish to stress the importance that companies are held to the standards set up by the UN Guiding Principles on Business and Human Rights (UNGPs), providing an authoritative global standard for preventing and addressing adverse human rights impacts linked to business activity. While the UNGPs have been endorsed by the Human Rights Council in Resolution 17/4 of 16 June 2011,[44] they are not formally legally binding. However, they represent an important step towards matching the impact of businesses on human rights with corresponding levels of corporate responsibility.[45] They also represent the direction of legal obligations, as soft law norms that may crystalize to hard law obligation over time and use. They are being recognized, accepted and implemented by a growing number of private companies.[46]

The Special Rapporteurs express their concern that the current draft of the text does not put sufficient emphasis on the human rights responsibilities of hosting service providers, especially as these are active in areas traditionally ascribed to States, such as by exercising quasi-regulative, quasi-enforcement and quasi-adjudicative functions in the context of the fight against terrorism. Their activity is also proactively being enabled and supported by States.

The Special Rapporteurs appreciate that the draft Regulation requires hosting service providers to establish "effective and accessible" complaint mechanisms (Article 10), imposes improved transparency obligations (Article 8) and mandates the preservation of removed or disabled content and related data (Article 7). They however express concern that relevant provisions are not framed in terms of human rights responsibilities incumbent upon companies. Moreover, the Proposal does not require companies to develop their terms of service and community standards as well as relevant policies with due consideration to human rights norms and standards.

In line with the 'respect, protect, remedy' framework set out under the UNGPs, companies should provide users with clear guidance on the circumstances under which content may be blocked, removed or restricted or their access to a service restricted or terminated. Policies regulating conduct on the platform must be set out in clear and accessible language and be sufficiently detailed to allow users to foresee the consequences of their use of the platform and have the option to adjust their conduct

[43] See, for example A/RES/72/284.
[44] A/HRC/17/4.
[45] A/HRC/35/22, para. 45; A/HRC/38/35, para. 11.
[46] See "Article 19: Defending freedom of expression and information" [independent organization], "Public interest, private infrastructure: an analysis of the barriers and drivers for adoption human rights standards in the Internet infrastructure industry", 5 June 2018, p. 14, available at https://www.article19.org/wp-content/uploads/2018/06/HRIA-report-UNGP_5.6.pdf.

accordingly. Companies should also regularly publish examples of "specific and representative cases" that illustrate how they resolve hard questions about the interpretation and enforcement of their policies, or significant developments in such interpretation and enforcement.[47] Furthermore, transparency reporting should include granular data on the volume and types of requests they receive (including private requests and referrals from government agencies), actions taken, the volume and types of users' appeals, response times and the rate at which such appeals are granted.[48]

Procedures set up to address user violations need to incorporate adequate safeguards against arbitrary or erroneous decisions. This implies setting up internal accountability mechanisms for the implementation of relevant policies[49] and having processes in place that enable the remediation of adverse human rights impacts that the company caused or contributed to.[50] In this sense, operational-level grievance mechanisms that are accessible, user-friendly and transparent, may be an effective means to ensure access to remedies to stakeholders whose legitimate interests have been infringed upon by the company, including users of the company's products and services.[51] In cases of content restriction or removal, affected users should be informed of the reasons for such measures.[52] Users should also be informed of any available remedies, the right to challenge the removal, blocking or filtering of content or blocking or suspension of user accounts.[53] Removed content and account information should be preserved. This is important both in case blocking, suspension or removal has been made erroneously as well as if such information may be needed as evidence of criminal conduct for a potential investigation. Given the volume of complaints and requests for appeals they handle, companies should also explore "scalable solutions such as company-specific or industry-wide ombudsman programmes."[54]

III. CONCLUSIONS AND RECOMMENDATIONS

Terrorism poses a serious challenge to the very tenets of the rule of law, the protection of human rights and their effective implementation. Effectively combatting terrorism and ensuring respect for human rights are not competing but complementary and mutually reinforcing goals, as it has been unanimously recognized by the UN General Assembly in the Global Counter-Terrorism Strategy.[55] Moreover, relevant provisions of Security Council resolutions 1373 (2001), 1456 (2003), 1566 (2004), 1624 (2005), 2178 (2014), 2341 (2017), 2354 (2017), 2368 (2017), 2370 (2017), 2395 (2017) and 2396 (2017); as well as Human Rights Council resolution 35/34 and General

47 A/HRC/38/35, paras. 62 – 63.
48 *Id.*, paras. 39 – 40.
49 UNGPs, Principles 22, 29 and 31.
50 See Office of the High Commissioner for Human Rights, *The Corporate Responsibility to Respect Human Rights. An Interpretative Guide* (2012), Section III.
51 In accordance with Principle 31, such grievance mechanisms can be considered effective if they are 1) legitimate, 2) accessible, 3) predictable, 4) equitable, 5) transparent, 6) rights-compatible, 7) a source of continuous learning and 8) based on engagement and dialogue.
52 A/HRC/38/35, para. 37.
53 *Id.*, paras. 37 – 38.
54 *Id.*, para. 58.
55 A/HRC/60/288.

Assembly resolutions 49/60, 51/210, 72/123 and 72/180 require that any measures taken to combat terrorism and violent extremism, including incitement of and support for terrorist acts, comply with States' obligations under international law, in particular international human rights law, refugee law, and international humanitarian law.

Respect for human rights and the rule of law must be the bedrock of the global fight against terrorism, and beyond rhetoric this principle must be reflected in practice, procedure and institutional culture. This requires human rights benchmarking and both *a priori* and *a posteriori* impact analysis as well as adequate oversight. In this vein, the Special Rapporteurs express concern that this new legislative initiative comes before the first assessment of the impact of Directive 2017/541, including of its implications on fundamental freedoms, to be prepared by the Commission by 2021. This is even more consequential considering that there has been no *a priori* impact assessment in regards of the Directive.

In light of the above observations, we urge that the following recommendations are implemented with the view of ensuring that the Regulation is brought in line with human rights norms and standards:

a) Ensure that the definition of terrorist content is narrowly construed to guarantee that measures taken pursuant to it do not unduly interfere with human rights. The Special Rapporteurs recommend that the model definitions developed by the mandate of the Special Rapporteur on counter-terrorism and human rights are duly considered in this respect;

b) Ensure that competent authorities designated by Member States benefit from institutionally embedded human rights expertise and that their decisions taken pursuant to the Regulation are subject to independent review, ideally of judicial nature;

c) Amend the draft Regulation to ensure that hosting service providers are only required to remove or disable content following an order by an independent and impartial authority;

d) Ensure transparency of measures taken pursuant to the Regulation to the maximum extent feasible, including those taken by Member State and Union authorities;

e) Define companies' human rights responsibilities in line with the 'respect, protect, remedy' framework set out under the UN Guiding Principles on Business and Human Rights, in particular by requiring a human rights approach to developing terms of service and community standards as well as policies governing access to and use of their platform.

f) Ensure that the collection and processing of all personal data carried out in furtherance of the Regulation which does not fall under the scope of Directive (EU) 2016/680 on the protection of natural persons with regard to the processing

of personal data by competent authorities for the purpose of law enforcement, or under the scope of the EU General Data Protection Regulation (GDPR), especially when such data is collected or processed for national security purposes, is done in accordance with the principles of legality, necessity and proportionality; as established by article 9 of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108).

Thank you in advance for the consideration of our views. Our mandates would be happy to continue the dialogue on the Regulation on preventing the dissemination of terrorist content online as it progresses through the legislative procedure.

This communication, as a comment on pending or recently adopted legislation, regulations or policies, and any response received from the European Union will be made public via the communications reporting website within 48 hours. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

Please accept, Excellency, the assurances of our highest consideration.

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Joseph Cannataci
Special Rapporteur on the right to privacy

Fionnuala Ní Aoláin
Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism