Vol. 92 issue 2, 2021

RIDP

Gert Vermeulen,
Wannes Bellaert *(Eds.)*

EU Criminal Policy: Advances and Challenges

Revue Internationale de Droit Pénal
International Review of Penal Law
Revista internacional de Derecho Penal
Международное обозрение уголовного права
刑事法律国际评论
المجلة الدولية للقانون الجنائي
Revista Internacional de Direito Penal
Rivista internazionale di diritto penale
Internationale Revue für Strafrecht

IRCP

MAKLU

AIDP – Association Internationale de Droit Pénal | The International Association of Penal Law is the oldest association of specialists in penal law in the world. Since 1924, it is dedicated to the scientific study of criminal law and covers: (1) criminal policy and codification of penal law, (2) comparative criminal law, (3) international criminal law (incl. specialization in international criminal justice) and (4) human rights in the administration of criminal justice. The Association's website provides further information (http://www.penal.org).

RIDP – Revue Internationale de Droit Pénal | The International Review of Penal Law is the primary publication medium and core scientific output of the Association. It seeks to contribute to the development of ideas, knowledge, and practices in the field of penal sciences. Combining international and comparative perspectives, the RIDP covers criminal law theory and philosophy, general principles of criminal law, special criminal law, criminal procedure, and international criminal law. The RIDP is published twice a year. Typically, issues are linked to the Association's core scientific activities, i.e. the AIDP conferences, Young Penalist conferences, world conferences or, every five years, the International Congress of Penal Law. Occasionally, issues will be dedicated to a single, topical scientific theme, validated by the Scientific Committee of the Association, comprising high-quality papers which have been either presented and discussed in small-scale expert colloquia or selected following an open call for papers. The RIDP is published in English only.

Peer review: All contributions are subject to double-layered peer review. The primary scientific and peer review responsibility for all issues lies with the designated Scientific Editor(s). The additional scientific quality control is carried out by the Executive Committee of the Editorial Board, which may turn to the Committee of Reviewers for supplementary peer review.

ISSN – 0223-5404
ISBN 978-90-466-1134-0
D/2022/1997/1
NUR 824
BISAC LAW026000
Theme: LNF, LAR

Maklu- Publishers
Somersstraat 13/15, 2018 Antwerpen, Belgium, info@maklu.be
Koninginnelaan 96, 7315 EB Apeldoorn, The Netherlands, info@maklu.nl
www.maklu.eu

USA & Canada
International Specialized Book Services
920 NE 58th Ave., Suite 300, Portland, OR 97213-3786, orders@isbs.com, www.isbs.com

Editorial Board

Summary

THE END OF TERRORIST CONTENT ONLINE?

By Wannes Bellaert,[*] Visara Selimi[**] and Robin Gouwy[***]

Abstract

Over time, the EU has taken several initiatives to tackle terrorist content, in addition to its historically well-developed counter terrorism criminal policy. While notice and voluntary take-down procedures for malicious terrorist content online have for years been facilitated and initiated by the Europol-based EU Internet Referral Unit (EU IRU) and the network of Member State level IRUs, the EU has decided to introduce a more compelling system upon providers offering services in the EU. The Terrorist Content Online Regulation, adopted mid-2021, grants the Member States' competent authorities the power to issue removal orders to service providers, requiring them to remove terrorist content or disable access to it in all Member States. While its objective may be justified, its impact on the right to free speech is undeniable.

1 Introduction

In 2015 the Commission launched the EU Internet Forum.[1] The intention was to bring around the table IT-companies, law enforcement authorities and civil society. The main objective was to address the rise of terrorist propaganda. At the same time, the Council instructed Europol to change its 'check the web' project into an EU Internet Referral Unit (EU IRU). Additionally, each Member State was asked to create a National Unit to complement the EU IRU at Europol's level.[2] Both in 2016 and 2017, the Commission published documents calling upon service providers to act more decisive regarding terrorist content online.[3] In 2017, the Commission even published guidance on the issue of illegal content online including terrorism.[4] This guidance was the result of the June European Council summit which called on tech companies to create new tools and even opened the door for EU legislation 'if necessary'.[5] The 2017 communication would not prove to be the last non-legislative measure of the Commission, as it adopted a recommendation

[*] PhD Researcher and Academic Assistant, Institute for International Research on Criminal Policy (IRCP), Ghent University. For correspondence: <wannes.bellaert@ugent.be>.

[**] Projectleader and thematic coordinator transversal security themes, Belgian Federal Public Service of interior affairs, security and prevention. For correspondence: <visara.selimi96@gmail.com>.

[***] Accredited Parliamentary Assistant, European Parliament. For correspondence: <gouwyrobin96@gmail.com>.

[1] Commission, 'European agenda on security' COM(2015) 185 final, 13.

[2] Council Conclusions 6606/15 Fight against terrorism: follow-up to the statement of 12 February by the Members of the European Council and to the Riga Joint Statement of 29 January by the Ministers of Justice and Home Affairs of the EU [2015], 4-5.

[3] Commission, 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe 25 May 2016' Com(2016) 288 final; Commission, 'The Mid-Term Review on the implementation of the Digital Single Market Strategy' COM(2017) 228 final

[4] Commission, 'Tackling Illegal Content Online' COM(2017) 555 final.

[5] European Council Conclusions 8/17 [2017], 2.

in 2018 on measures to effectively tackle illegal content online.[6] In the end, it would be the European Council which called upon the Commission to present a legislative proposal on the dissemination of terrorist content online.[7] This would be the result of the ongoing terrorist attacks in several Member States, the presence of the content online, but also 'by continued concern about the role of the internet in aiding terrorist organisations to pursue and fulfil their objectives to radicalise and to recruit, to facilitate and direct terrorist activity'.[8]

In 2018, the Commission proposed a new Regulation Addressing the Dissemination of Terrorist Content Online.[9] The initiative came on the heels of the European Parliament calling on the Commission to present proposals 'to strengthen measures to tackle illegal and harmful content'[10] and similar calls made by several Member States. On the 29th of April 2021, the new regulation was adopted. The new rules apply from the 7th of June 2022.[11]

The competent authorities in the Member States will have the power to issue removal orders to the service providers, requiring them to remove terrorist content or disable access to it in all Member States. Internet platforms will then have to remove or disable access to the content within one hour. The rules will apply to all providers offering services in the EU, whether they have their main establishment in one of the Member States or not. According to the Council of the European Union, the legislation provides for a clear scope and a uniform definition of terrorist content in order to fully respect fundamental rights. It should also include effective remedies both for users whose content has been removed and for service providers to submit a complaint.[12]

Whilst recognizing the challenging regulatory context and the laudable goal of using legal tools to prevent misuse of internet platforms in the context of terrorism, the Terrorist Content Online regulation raises concerns about free speech. In the first part, the terrorist regulation online content is analysed with special attention to the scope of application,

---

[6] Commission recommendation C(2018)1177 final of 1 March 2018 on measures to effectively tackle illegal content online [2018].

[7] European Council conclusions 9/18, point 13; Commission, 'Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online' COM(2018) 640 final.

[8] Commission, 'Staff Working Document Impact Assessment on proposal for a regulation on preventing the dissemination of terrorist content online' SWD(2018) 408 final, 2.

[9] European Commission, 'Security Union: Commission welcomes political agreement on removing terrorist content online', *(European Commission,* 10 December 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2372> accessed 27 August 2021.

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

[11] COM(2018) 640 final, 2.

[12] Council, 'Terrorist content online: Council adopts new rules' (*Concilium*, 16 March 2021) <www.consilium.europa.eu/en/press/press-releases/2021/03/16/terrorist-content-online-council-adopts-new-rules/> accessed 24 April 2021.

comparing the proposal with the Regulation. In the second part, the competent authorities allocated to issue removal orders and decisions are discussed. In the third part, the compatibility of the regulation with human rights is assessed. In the fourth part, the applicability of the regulation on the surface web is examined. Furthermore, in the fifth part, the applicability is further elaborated by a case example, about Islamic State propaganda on media platforms. Lastly, a conclusion integrates the outcome of the analysis.

2 Terrorist Content Online Regulation: Scope of Application

Through this new regulation the EU is working to stop terrorists from using the internet to radicalise, recruit and incite to violence. The objective of the legislative measure is to facilitate a quick removal of terrorist content online and to establish a common instrument for all Member States to this effect.

The regulation is applicable to hosting service providers offering their services in the EU irrespective of their main establishment. Besides the previous voluntary cooperation with the hosting service providers, the new set of rules will provide additional tools for member states to be able to respond swiftly to online terrorist content where necessary, by means of removal orders.

The aforementioned removal orders will be issued by competent authorities in the Member States and will be directed to the service provider(s). The service provider in case will then be obliged to remove to content or disable access to it in all Member States. These measures will have to be in place within the hour.

Further, the hosting service providers exposed to terrorist content are obliged to take specific measures to address the misuse of their services and to protect them against such usage. The choice considering which measures to be taken, is left to the discretion of the hosting service providers.

2.1 Defining terrorist content

2.1.1 Commission proposal

On the 12 September 2018, the Commission launched a proposal for a Regulation on preventing the dissemination of terrorist content online to complement Directive 2017/541 on combating terrorism. The Commission provided an outlined definition on the notion of 'terrorist content'. The outline provided four categories of what can be perceived 'terrorist content'. In what follows, an analysis will be conducted on Article 2(5) - on the definition of terrorist content - of the proposal of the European Commission and on every individual limb of Article 2(5) of the proposal.

Firstly, Article 2(5) of the proposal does not require any form of intention, which is in contradiction with the Directive on combatting terrorism. In this manner, the scope of the proposal is broader than the one of the Directive. By excluding the intent element, some authors suggested that also other online content could resort under the definition

and thereby be removed from the internet. Could academic work or a news item be removed if they would resort under the definition of terrorist content? In its Decision of 2018, the European Court of Human Rights (ECtHR) implicitly defined terrorist content. In it, there is no element indicating that there is need of some form of intention.[13] The Court of Justice (CJEU) in the same case provided for an interpretation of 'incitement to hatred'. The CJEU concluded that incitement requires an element of intention, but it did not express itself further.[14] 'Inciting' is only mentioned once under Article 2(5)(a) of the proposal. In subsequent parts the proposal refers to 'advocating', 'encouraging', 'promoting' and 'instructing'. Some of these could entail an intentional element, nonetheless this is not a necessity.

Another comment regarding the intentional element is of the interest. In the current directive on combatting terrorism, there is a need for an intentional element to be present, while the proposal does not require such an element. There seems no reasonable explanation of why internet content should be treated more severely, as there is no intention required, while terrorist conduct is treated less severely, as there is an intentional element. In fact, the directive and the proposal even contradict one another. The directive, in its article on public provocation to commit a terrorist offence, clearly requires an intentional element, while the proposal makes no notice of it. An explanation of the difference can perhaps be found in the difference in legal basis of the proposal and the directive. Nonetheless, consistency between related legislation is required, as it ensures legal certainty. Even though there is a different legal basis, if in practice public prosecutors would prosecute persons for their online content, there would be no distinction, making it all the more needed to have consistency between different pieces of legislation, which is currently lacking.

In addition, some authors have stated that the concept of 'terrorist content' is missing an element. They propose to add the word 'illegal', making it 'illegal terrorist content'. [15] European Digital Rights (EDRi) argues that in this way certain materials were blocked by online service providers, even though the content was 'nasty but not illegal'.[16] However, it seems like the foregoing point on intention and the comment on illegal content go hand in hand. The example put forward by EDRi is not done with the intention of glorifying terrorist conduct. Correcting the problem of a lacking intention by adding the word 'illegal' creates two problems. Firstly, it seems to suggest that there can be 'legal' and 'illegal' terrorist content. Secondly, the way EDRi phrases it, terrorist content can only be considered illegal terrorist content if it is done intentionally. This could have

[13] *Roj TV A/S v. Denmark* App no 24683/14 (ECtHR, 17 April 2018), para 46-47.
[14] Joined Cases C-244/10, C-245/10 Mesopotamia Broadcast A/S METV and Roj TV A/S v. Bundesrepublik Germany [2011] ECR I-08777.
[15] EDRi, 'EDRi Amendments on the proposal for a Regulation to prevent the dissemination of terrorist content online' (2019) < 20190116_EDRi_ProposalForAms.pdf> accessed 24 April 2021.
[16] EDRi, 'All Cops Are Blind? Context in terrorist content online' (*EDRI*, 13 February 2019) <All Cops Are Blind? Context in terrorist content online - European Digital Rights (EDRi)> accessed 24 April 2021.

unintended and undesired consequences, as it would entail that a person could unintentionally commission terrorist offences within the meaning of directive 2017/541, but, in view of the unintentional element, the content would not be illegal, thereby the content could not be removed. Criticism regarding the lack of objectivity of the proposal was made by some authors, but the changes proposed by EDRi would make it entirely subjective, as the question would become what is illegal and what is legal. Thereby, every person acting in an involuntarily manner would be exonerated, this would once again demonstrate a lack of objectivity which could be a problem, as doubts could arise on the intention of a person or the absence thereof.

Although EDRi provides criticism demonstrating the risk for fundamental rights, certainly the right to free speech. Narrowing the scope of the concept 'terrorist content' cannot be considered the solution, as implementation is stil required either by persons or algorithms, which requires a form of consistency. The rules should be clearer to provide consistency between the different Member States in implementing the regulation, but the higher the number of conditions, the harder it becomes to remove content, while the fewer conditions, the easier for some to abuse the regulation.

The first limb of Article 2(5) of the proposal perceives something to be terrorist content in case of 'inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed'.[17] The United Nations special rapporteurs have raised questions on the word 'glorifying'. They consider it 'insufficiently defined', as no indication on how to interpret the word is provided .[18] On top of that, the limb also includes the concept of 'causing a danger'. Once again there is no indication on how to interpret this concept. Therefore, the first limb would on two occasions – 'glorifying' and 'causing danger' – leave the implementation completely up to the competent national authorities. As removing content relates to the right to free speech, a limitation to such right should comply with the legality test. As limiting a right should be based upon law, it is a prerequisite that the law is foreseeable. According to the Fundamental Rights Agency of the EU (FRA), 'foreseeability requires an act to be formulated with sufficient precision to enable the citizen to adapt his or her behaviour to the norm'.[19] If a citizen is unaware what should it mean to glorify or to cause a danger, then this rule cannot be compatible with the limitation test in Article 51(1) of the Charter of Fundamental Rights (CFR).

The second limb of Article 2(5) of the proposal states that '*encouraging the contribution to terrorist offences'* is part of terrorist content. The FRA considers this the most 'ambiguous description of terrorist content', as it does not seem to accord with any specific offence under the directive on combatting terrorism. In addition, the FRA complains that the

[17] COM(2018) 640 final.

[18] Special Rapporteur David Kaye, Special Rapporteur Joseph Cannataci and Fionnuala Ni Aoláin, 'Comments on the Proposal for a Regulation on preventing the dissemination of terrorist content online to complement Directive 2017/541 on combating terrorism' (7 December 2018) OL OTH 71/2018.

[19] Fundamental Rights Agency, Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level – Guidance (Publicatino Office of the European Union, 2020), 71.

term 'encouraging' is not defined in the proposal and thereby leaving it open to 'varying interpretations based on subjective evaluations'.[20] The foregoing makes it possible that this will result in 'disproportionate interferences with the freedom of expression'.[21] The UN rapporteurs conclude that this paragraph broadens the scope of what would be considered terrorism. Even the directive on combatting terrorism leaves some margin of discretion including certain actions, as it states that 'funding its activities in any way' is considered an offence related to a terrorist group. Thereby, providing human recourses to a terrorist group in order to commit terrorist offences can be perceived as a form of funding. The foregoing interpretation of the directive provides the Member States with unlimited possibilities of including certain actions. As indicated in the foregoing comments and as is the case here, there is room for manoeuvring for the Member States, which risks jeopardising the objective of harmonisation.

The third limb of Article 2(5) of the proposal mentions the following as terrorist content: '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'. According to the FRA, the scope of this limb is broader than its counterpart in the directive on combatting terrorism.[22] As the meaning of 'promoting' is unclear and the requirement of intent is lacking, it creates the possibility of removing everything, which correlates withterrorism. Therefore, it risks violatingthe right to free speech in its essence, which is an irregular limitation of that right.[23]

The fourth limb of Article 2(5) of the proposal includes 'instructing on methods or techniques for the purpose of committing terrorist offences' in the definition of terrorist content. In the FRA's view, the proposal when used 'outside of the framework of a criminal trial, may […] significantly increase the likelihood of capturing also technical, marketing or training materials which are not related to terrorism'.[24] Once again, the proposal fails to define certain words such as 'methods' and 'techniques'. In this way, the proposal provides a possibility for diverging views between the Member States when implementing the Regulation.

The Commission's proposal has laid the basis for the new regulation on terrorist content online. There are numerous problems, which should be addressed to prevent failure of harmonisation, disunity between Member States and abuse of the Regulation and thereby disproportionate limitation of certain fundamental rights.

[20] FRA Opinion 2/19 on Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications [2019], 18.
[21] Ibid, 17.
[22] Ibid.
[23] Charter of fundamental Rigths, Article 52 (1).
[24] Ibid, 19.

2.1.2 *Regulation from the European Parliament and Council*

On the 29th of April 2021, the Regulation addressing the dissemination of terrorist content online was adopted by the European Parliament and the Council. The regulation does not explicitly require an intentional element when it concerns terrorist content. Although intention was not required explicitly, it can be read into the article based upon the choice of words made by the legislator.[25] The legislator uses the word 'incites', which, as explained by the CJEU, entails an element of intent, and solicitation.[26] However, the recitals seem to cast some doubt on the foregoing. As glorifying terrorist activities, including 'disseminating material depicting a terrorist activity', can be considered terrorist content as well, it seems no intentional element is needed in the latter cases.[27] In this manner, the door is opened to remove content which is only glorification in the eyes of the national authorities. Likewise, the regulation is overstepping what is foreseen by the directive. The latter only imposed an obligation upon the Member States to take appropriate measures in case of intentional incitement, while the regulation as mentioned before seems to go beyond.[28]

Worth noticing is that the legislator did not alter the name of the concept – terrorist content - and thereby prevented the possible discussing of legal and illegal terrorist content. In addition, the legislator stated that artistic, journalistic, academic and research related works disseminated to the public in order to prevent or counter terrorism will not be considered terrorist content.[29] Even though this seems an appropriate level of protection, there is no definition provided on what artistic, journalistic, academic and research related works are. On top of that, it is unclear for national authorities when they should perceive something as done with the objective preventing or countering terrorism and when the content is created with the objective of supporting terrorism. For the moment, a common European Union all-round list of terrorist groups is lacking, making it possible for Member States to have a different perception on what specific group(s) or person(s) is/are called terrorists. Both the recital and provision on the different sets of works were introduced to counter the criticism that was mentioned before, however, it remains to be seen whether all the loose ends will prevent abuse of the regulation. It is likely that this provision will become subject of debate and will have to be clarified by the CJEU.

Luckily, the legislator has been aware of certain of the possible foregoing problems. Therefore, an assessment will have to be conducted by the national authorities on whether something can be considered terrorist content. However, in the regulation there

---

[25] European Parliament and Council Regulation 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L 172/79, Article 2(7).

[26] Joined Cases C-244/10, C-245/10 *Mesopotamia Broadcast A/S METV and Roj TV A/S v. Germany* [2011] ECR I-08777, para 41.

[27] Regulation 2021/784, recital 11.

[28] European Parliament and Council Directive 2017/541 of 15 March 2017 on combatting terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, Article 5.

[29] Regulation 2021/784, Article 1(3) and recital 12.

is no article provided for that strives towards transparency on this assessment. Only Article 10 obliges the service provider to make the reasons for its decisions known to an individual after a complaint from that individual. The regulation does not stipulate that the reasons for the decision should be the individual motivation for that specific complainant. Thereby, an assessment is made without any form of control. Even though there still is the option of going to court, who will do so?

Another element worth nothing in the regulation is the addition of a new element that can be considered terrorist content. The legislator added a subparagraph e) which entails that also the threat of committing one of the acts foreseen in the directive on combatting terrorism is subject to the regulation. Thereby, the link between the directive and the regulation is reinforced.

The European legislator has asked the Member States to designate competent authorities to execute this regulation. Neither the proposal nor the regulation paymuch attention to them and do not explicitly require them to be independent.[30] The removal of terrorist content will be executed by an authority which could possibly be administrative, law enforcement or judicial.[31] The Regulation requires only that the authority executes their task in an 'objective and non-discriminatory manner' and 'shall not take nor seek instructions from any other body in relation' to the tasks it should carry out. Thismakes it possible to state that there is a lack of an independent authority, which is required in case of data protection. This could prove to be problematic, as the extreme right ideologies are on the rise, including within police and military ranks.[32] Additionally, there are certain Member States where the rule of law is under threat, making it hard to believe that the competent authorities in these Member States will operate in an objective and non-discriminatory manner. The foregoing could exploit certain problems indicated before regarding the scope of application of the regulation.

The Regulation made substantial changes in comparison to the proposal of the European Commission; some comments made upon the proposal were taken into consideration, while others were ignored. It can be concluded that the scope of application of the Regulation is clearer than the one of the proposal, by having removed multiple undefined words. The extension of the scope of the regulation by including threats is in line with the directive. Lastly, the competent authorities could prove to become a problem, as there is no explicit requirement of them being independent.

---

[30] 'European Union: independent judiciary and effective remedies must be at the core of the EU Regulation on "Terrorist Content Online", warns ICJ' (*International Commission of Jursits*, 7 December 2020) <European Union: independent judiciary and effective remedies must be at the core of the EU Regulation on "Terrorist Content Online", warns ICJ | International Commission of Jurists> accessed 24 April 2021.

[31] Regulation 2021/784, recital 35.

[32] Alexandra Brzozowski, 'Far-right terrorism bigger threat to West than Islamic State – study' (*Euractiv*, 25 November 2020) <Far-right terrorism bigger threat to West than Islamic State – study – EURACTIV.com> accessed 25 April 2021.

3 Competent Authority

3.1 Independent

Although it was discussed in the one of the foregoing paragraphs, what still needs to be further discussed isthe issue of the competent authorities. In its commentaries to the Members of the European Parliament, EDRi and several other non-profit organisations complained that the orders for removal would not be independent. If it were up to EDRi and the others, only courts or independent administrative authorities would be allowed to issue these orders or decisions for removal of certain online content.[33] The Commission in its proposal did not spend two lines on the competent authorities, demonstrating it was up to the Member States how they wanted to implement this. The Council, as representative of the Member States, proposed an entire new paragraph which, aside from the last sentence, became Article 13(2) of the Regulation.[34] The Parliament on the other hand only wanted to add a single sentence to the Commission's proposal, which included independence for the competent authority.[35] As a compromise, the European Parliament accepted the Council's wording, but removed the following sentence from the Council's proposed amendment: 'This shall not prevent supervision in accordance with national constitutional law.'

The question should be raised what the consequence is of the absence of the sentence of the Parliament – insisting on independence – and the removal of the sentence of the Council – on national supervision. In essence, the competent authority should be objective, act in a non-discriminatory fashion and 'shall neither take nor seek instructions from any other body'. The words 'objective' and 'non-discriminatory' are pleading for the impartiality of a certain actor, but what does it mean not to seek or take instructions?

The foregoing explains why the European Parliament was eager to remove the last sentence of the Council, as both the current last sentence and the one proposed by the Council seem incompatible. But what is meant with 'neither take nor seek instructions from any other body'? To answer this question, it is interesting to analyse what it means to be independent. In its 2010 case on the independence of the German Data protection authorities, the CJEU clarified that independent means 'a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure'.[36] In addition, the CJEU stated that concept of independence was clarified by adding 'may neither seek nor take instructions from anybody'. In ample

[33] 'Open letter: Civil society urges Member States to respect the principles of the law in Terrorist Content Online Regulation' (*EDRI,* 27 March 2020) <https://edri.org/our-work/open-letter-civil-society-urges-member-states-to-respect-the-principles-of-the-law-in-terrorist-content-online-regulation/> accessed 27 April 2021.

[34] Council note 12618/20 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissmenation of terrorist content online [2020].

[35] European Parliament Resolution on the proposal for a regulation of the European Parliament and of the Council on preventing the dissmenation of terrorist content online [2019], am. 110.

[36] Case C-518/07, *Commission v. Germany* [2010], para 18.

other legislative and treaty-based articles the phrase 'neither take nor seek instructions' is mentioned just before or after a sentence indicating the independence of a body.[37]

In contradiction to the case against Germany, where it was mentioned that the data protection authority should be 'complete[ly] independen[t]', the Regulation mentions 'any other body'. This entails any other human, legal, non-governmental or state body. The foregoing sentence should not mean that the competent authority is excluded from judicial intervention by a national court or the Court of Justice, as the competent authority still has to act in accordance with the rule of law. Therefore, the competent authorities that each individual Member States has to establish should be independent. Options to establish such an independent competent authority are provided for in the GDPR. Fact that this could entail a law enforcement authority does not withstand this, as even the executive director of Europol should act independently.

3.2 Cooperation

Over the years, the EU has created several directives and regulations in which authorities or entities were tasked with executing certain specificities for the directive or regulation. On multiple occasions cooperation or coordination was established to allow the different entities to keep in touch with each other and allow the implementation to happen in a more consistent manner. A similar mechanism is included in the Regulation. 'Competent authorities shall exchange information, coordinate and cooperate with each other' is the sentencementioned in the Regulation. In the next part of the sentence the Regulation makes it possible to use Europol to prevent duplication of work and to create some form of coordination.

Aside from Europol, the European Commission was tasked to ensure cooperation and coordination among the different Member States. However, in both instances it seems there will be limited contact between the different competent authorities themselves. As the orders and decisions can have cross border effects, there is the need to have a uniform application of the regulation to prevent disputes between Member States on the scope of the regulation. Allowing an EU entity, consisting of all the national competent authorites, to create some guidance, a common stance on the scope or even binding measures could prevent these disputes from arising.

In the past, the legislator created similar sorts of boards, group or entities bringing together a representative from every Member State. In the GDPR, the European Data Protection Board (EDPB) is created and in 2020 the European Commission for the first time

[37] The European Central Bank (Article 130 TFEU iuncto Article 7 Protocl 4 on the statute of the European Central Bank), Court of Auditors (Article 286 TFEU), National Supervisory Authority on data (Article 51 GDPR), Ombudsman (Article 228(3) TFEU), European Commission (Article 245 TFEU), OLAF (Regulation 883/2013 on both the supervisory committee and the controller of procedural guarantees), European Economic and Social Committee and the Committee of the Regions (Article 300 TFEU), Data Protection Officer (Article 44(3) iuncto Article 45(1)(b) Regulation 2016/679), Europol Cooperation Board (Article 45 Regulation 2016/794).

presented an evaluation report. In it, the Commission concluded that the EDPB has contributed to the application of the GDPR but added that it could do more in terms of cooperation and encouragement for a uniform application.[38]

Both issues – preventing disputes and a common view – will prove to be essential to ensure a proper implementation and application of the terrorist content online regulation. Establishing a similar board to the GDPR in this case, could help preventing and addressing problems related to uniform application and cross-border effects of orders and decisions. However, the question should be raised whether it is worth the effort of trying to establish such an entity if Member States are possibly unwilling to cooperate. Although the Regulation is adopted under the Internal Market competence, terrorism is not diminished to a minor issue because of it. Terrorism is considered an issue of national security, making the willingness of (certain) Member States possibly limited as they don't want any further limitation based upon guidance or even binding measures.

4 Right to Access to Information and Freedom of Opinion and Expression

If the foregoing line of reasoning on the independence would be mistaken and the competent authorities would not have to be independent, then an analysis of the limitations imposed upon certain fundamental rights is required. These rights and freedoms are included in the Charter and are applicable in all instances governed by EU law.[39] Most fundamental rights can be subject to limitationsin accordance with the requirements expressed in the Charter, i.e., the limitations should be provided by law, respect the essence of these rights and freedoms, pursue a legitimate goal and be proportionate.[40]

For a law to impose limitations on a fundamental right, it should be foreseeable and accessible. The former means that a person should be able to predict the consequences of the legislation at hand. Therefore, the legislation should be precise and predictable. Of course, a piece of legislation must be implemented and therefore providing the authorities with a certain discretion. However, limits should be imposed upon this discretion and measures should be adopted to counter possible abuses. As the regulation requires ongoing implementation by the competent authorities, there is a clear risk of possible abuses. There is no alternative for a person than to go to the national court of the Member State, the competent authority of which issued the removal order. As there is no requirement for these authorities to be independent and the independence of the courts and tribunals in certain Member States is under threat, what is there to prevent abuse? Indeed, the Regulation provides for the option for the service provider not to comply with the order or the decision and go to court to challenge the order or the decision; however, there is also the possibility for the Member States to impose a fine upon the service pro-

[38] Commission, 'The digital transition on Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation', COM(2020) 264 final, 15.
[39] Case C-617/10 Aklagaren v. Hans Akerberg Fransson [2013].
[40] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, Article 52(1).

vider if they do not comply. Although, a fine should be effective, proportionate and dissuasive, the likelihood of Hosting Service Providers not complying with an order or a decision is becoming less likely. On this note, it is unclear what should be understood under the notion of dissuasive. It could potentially open the door to more severe fines. On top of that, the Regulation considers that a fine can be proportionate not only when systematic problems arise but also in an individual case. Thereby, actual opposition by Hosting Service Providers becomes almost unthinkable. The idea of opposition should perhaps even be excluded entirely in case of automatic processing of orders or decisions. The finale solution will most likely have to be offered by individuals going to court, but, as already stipulated, it will be up to the individual to perhaps exhaust all the legal remedies in a Member States to ask a preliminary reference to the CJEU, in case the national courts can no longer be considered independent. This could make the procedure last for several years before justice can, not even will, be done. Who is willing to have judicial struggles for several years? Is this what is called an adequate mechanism against abuse?

Aside from respecting the essence of right and having a legitimate goal, a limitation should also be proportionate. This requires a measure not only to be proportionate but also appropriate and necessary. Stating this measure is necessary to prevent further terrorist content seems obvious, but the question should be whether the measure is proportionate. By whom should the actions in the definition on 'terrorist content' be committed to be considered an act of terror within the meaning of terrorist content? Although this regulation is a clear response to the terrorist attacks over the past years, which were in origin Jihadi terrorist attacks, this does not prevent it from being used in other situations.[41] Extreme right terrorism is on the rise.[42] Making use of the Regulation for these forms of terrorism is legal, but it raises additional problems. An interesting question in this regard, considering tendencies in some Member States, is: when is someone acting as a terrorist, in accordance with this regulation, and when it a person merely acting as a political opponent? The answer points to Article 3 of the Directive on combatting terrorism. Although this was not discussed in the first part, but even the definition in that Directive provides some leeway to include persons who might not be involved in any terrorist crimes. On top of that, the second paragraph uses words which provide for sufficient margin of discretion. Recently, the speaker of the Hungarian Parliament said to the Secret Service of Hungary that the opposition is the biggest threat to national security.[43] If the competent authority is not independent and the opposition makes a statement during elections campaign in 2022, will these be removed as they form a threat to national security which can easily be framed under Article 3 part 2 under c of the Di-

[41] COM(2018) 640 final, 1.

[42] Alexandra Brzozowski, 'Far-right terrorism bigger threat to West than Islamic State – study' (*Euractiv*, 25 November 2020) <Far-right terrorism bigger threat to West than Islamic State – study – Euractiv.com> accessed 25 April 2021.

[43] Vlagyiszlav Makszimov, 'Fidesz speaker to secret services: opposition is biggest threat to national security' (Euractiv, 29 November 2021) <Fidesz speaker to secret services: opposition is biggest threat to national security – Euractiv.com> accessed 30 November 2021.

rective on combatting terrorism? As the definitions included in the directive on combatting terrorism provide leeway for abuses for autocratic regimes in the EU, the regulation fails to provide sufficient shackles to prevent abuse. Thereby, it is impossible to conclude in any other manner than the disproportionalityof the Regulation, as it violates the right to free speech in an excessive manner.

Preventing abuse was the initial starting point. Both regarding the legality and the proportionality requirement, this has not been succeeded. The rights of persons can be limited, but the extent to which should be foreseeable and proportionate. On both occasions the door is open towards abusing the system created by the EU. Independent authorities could prevent interference from the governments, making both problems disappear. Why should data protection be ensured by independent authorities and the right to information and freedom of opinion and expression wouldn't? Are all human rights not indivisible and interdependent?

5 Key Elements of the Regulation

In this section, the paper analyses a few key elements of the Regulation. First, the encouragement to take 'proactive measures', such as automated tools, to prevent terrorist content from being uploaded will be examined. Afterwards, the swift removals across borders will be analysed. Finally, possible bottlenecks that may arise will also be identified when discussing the key elements.

5.1 Proactive measures

The Regulation encourages companies to take 'proactive measures' to prevent terrorist content from being uploaded on their platforms.[44] The Regulation incentivises online platforms to use automated tools, like upload filters and remove content that is deemed to be of a 'terrorist' nature.[45] More specifically, the regulation states that every hosting service provider needs to 'take specific measures to protect its services against the dissemination to the public of terrorist content.'[46] The regulation lists some examples, including technical means and user-flagging.

Furthermore, any other mechanisms to increase the awareness of terrorist content on its services, such as mechanisms for user moderation and any other measure that the hosting service provider considers to be appropriate to address the availability of terrorist content on its services.[47] These specific measures may play out in content moderation tools and policies. Nonetheless, some companies are not willing to devote unlimited resources to terrorist content. Consequently, there may be a chance that they are going to use 'technical means', such as machine learning algorithms and upload filters. For those

[44] Regulation 2021/784.
[45] Dia Kayyali, 'It's not too late for Members of European Parliament to vote no on the disastrous "Terrorist content" regulation' (*MNEMONIC,* 25 March 2021) <https://mnemonic.org/en/content-moderation/Mnemonic-joins-61-organisations-urging-EU-to-vote-no> accessed 23 April 2020.
[46] Regulation 2021/784, Article 5(2).
[47] Ibid.

companies this will be the best choice, as they are more cost-effective.[48] Nevertheless, these technical means can be error-prone and those errors can have a real cost.[49] Content recognition software continues to make mistakes.[50] The Impact Assessment document accompanying the initial proposal of the Regulation states that despite progress in the field, cases of misidentification of visual content continue to occur.[51]

This will further be elaborated with some examples. In June of 2017, Google instituted a machine-learning algorithm to 'more quickly identify and remove extremist and terrorism-related content'.[52] This technical means caused hundreds of thousands of videos being deleted. This included not only videos created by perpetrators of human rights abuses but also documentation of shellings by victims, and even videos of demonstrations.[53] Since Google started using machine-learning for content moderation, multiple other platforms have followed suit. In addition, some mistakes were also made by Facebook. At the start of the COVID-19 pandemic, platforms also greatly increased their use of automation. This sometimes led to nonsensical results.[54] It was determined that Facebook's AI was removing pandemic-related fundraisers for a brief period.[55] Another example is Facebook censoring Rohingya accounts of the genocide. Countless Rohingya refugees have tried to record the ethnic cleansing of their communities by turning to Facebook, the social network that promised to give a voice to the voiceless. Nevertheless, rather than finding solidarity, they faced censorship, as Facebook was deleting their stories and blocking their accounts by mistake.[56]

It is sometimes impossible for automation to differentiate between parody, satire, educational material and actual terrorist content. As we have seen above, there is a strong

---

[48] Dia Kayyali, 'It's not too late for Members of European Parliament to vote no on the disastrous "Terrorist content" regulation' (*MNEMONIC,* 25 March 2021) <https://mnemonic.org/en/content-moderation/Mnemonic-joins-61-organisations-urging-EU-to-vote-no> accessed 23 April 2020.

[49] Ibid.

[50] Aleksandra Kuczerawy, 'The proposed Regulation on preventing the dissemination of terrorist content online: safeguards and risks for freedom of expression' (2018) Center for Democracy and Technology < https://cdt.org/insights/research-paper-from-leuven-university-proposed-regulation-on-preventing-the-dissemination-of-terrorist-content-online/> accessed 24 April 2021.

[51] European Commission, Impact Assessment (n 33); K. O'Flaherty, 'YouTube keeps deleting evidence of Syrian chemical weapon attacks' (*WIRED,* 26 June 2018) <www.wired.co.uk/article/chemical- weapons-in-syria-youtube-algorithm-delete-video> accessed 24 April 2021.

[52] Kent Walker, 'Four steps we're taking today to fight terrorism online' (*Blog Google*, 18 June 2017) <www.blog.google/topics/google-europe/four-steps-were-taking-today-fight-online-terror/> accessed 24 April 2021.

[53] Ibid.

[54] Dia Kayyali, 'It's not too late for Members of European Parliament to vote no on the disastrous "Terrorist content" regulation' (*MNEMONIC,* 25 March 2021) <https://mnemonic.org/en/content-moderation/Mnemonic-joins-61-organisations-urging-EU-to-vote-no> accessed 23 April 2020.

[55] Ibid.

[56] Albert Fox Cahn, 'Why Is Facebook Censoring Rohingya Accounts of the Genocide?' (*Newsweek*, 2 October 2017) <www.newsweek.com/why-facebook-censoring-rohingya- accounts-genocide-675526> accessed 24 April 2021.

chance that mistakes are being made and news content or evidence of war crimes or maltreatment of minorities gets removed automatically. Consequently, harming our ability to get informed or freely express ourselves.[57] Nevertheless, the Regulation has put in place four requirements that need to be fulfilled.[58] First, they shall be effective in mitigating the level of exposure of the services of the hosting service provider to terrorist content. Second, they shall be targeted and ruminated. Third, they shall be applied in a manner that takes full account of the rights and legitimate interest of the users, in particular users' fundamental rights concerning freedom of expression and information, respect for private life and protection of personal data. Lastly, they shall be applied in a diligent and non-discriminatory manner.[59]

In addition, the regulation states that the hosting service provider should report to the competent authority on the specific measures in place in order to allow that authority to determine whether the measures are effective and proportionate and whether, if automated means are used, the hosting service provider has the necessary capacity for human oversight and verification.[60] Where specific measures involve the use of technical measures, appropriate and effective safeguards, in particular through human oversight and verification, shall be provided to ensure accuracy and to avoid the removal of material that is not terrorist content.[61] However, as set out by the example above, the conditions are not easy to fulfil, and human oversight may not always help with erroneous removals.

EDRi had already given critique on the proposal of the regulation by stating that without clear safeguards these systems could further the power imbalance between those who develop and use AI and those who are subject to them. This is why a strong AI regulation from the EU is needed.[62] It seems, however, that insuffiient safeguards were put into place in order to avoid this. The majority of requirements in the proposal naively rely on AI developers to implement technical solutions to complex social issues. Moreover, these complex issues are likely self-assessed by the companies themselves. In this way, the proposal enables a profitable market of unjust AI to be used for surveillance and discrimination.[63]

[57] 'Free Speech Advocates Urge EU Legislators to Vote 'No' to Automated Censorship Online' (*Liberties*, 25 March 2021) <www.liberties.eu/en/stories/terrorist-content-regulation-open-letter-to-meps/43410> accessed 24 April 2021.
[58] Regulation 2021/784, Article 5(3).
[59] Ibid.
[60] Regulation 2021/784, Article 7.
[61] Ibid, Article 5(3)
[62] EDRi, 'EU's AI proposal must go further to prevent surveillance and discrimination' (*EDRi*, 21 April 2021) <https://edri.org/our-work/eus-ai-proposal-must-go-further-to-prevent-surveillance-and-discrimination/> accessed 24 April 2021.
[63] Ibid.

Interesting to note is the recent news brought out by Frances Haugen, a whistle-blower who formerly worked at Facebook at the specific division civic integrity, tackling misinformation and hate crime. She unveiled that it is in Facebook's interest to have hate comments on Facebook, as they encourage people to spend more time on Facebook. She argued that it is against Facebook's interest to remove certain content for public security reasons.[64]

5.2 Swift removals across borders

Another key element of the Regulation is the possibility for Member States to issue swift removals across borders and aside from the comments made towards cooperation in point 3.2. The Regulation creates new requirements for hosting service providers. More specifically, they are obliged to remove content or disable access within one hour of having received a removal order from a competent authority.[65] Each Member State will be able to appoint the aforementioned competent authority. Systematic or persistent failure to meet the one-hour deadline could result in financial fees of up 4% of the company's global annual turnover.[66] Nevertheless, according to the Regulation, due account should be taken of the financial resources of the hosting service provider when determining the financial penalties. Moreover, the competent authority should consider whether the hosting service provider is a start-up or a micro, small or medium-sized enterprise, as defined in Commission[67] Recommendation 2003/361/EC.[68]

In addition, there have been some concerns in regard to the one-hour deadline. Whilst the regulation clarifies that its definition of 'terrorist content' is based on the Directive on Combatting Terrorism[69], it is believed that due to the risk of financial penalties, companies might remove content shared for journalistic and academic purposes.[70] Because of the short time limit, they may not be inclined to properly research the request. However, the Regulation clearly states that 'Member States should ensure that penalties imposed

---

[64] Luca Bertuzzi, 'Facebook Whisteblower calls on CEO Mark Zuckerberg to resign' (*Euractiv*, 5 November 2021 <www.euractiv.com/section/digital/news/facebook-whistleblower-calls-on-ceo-mark-zuckerberg-to-resign/> accessed 6 November 2021.

[65] Council, 'Terrorist content online: Council adopts new rules' (*Concilium*, 16 March 2021) <www.consilium.europa.eu/en/press/press-releases/2021/03/16/terrorist-content-online-council-adopts-new-rules/> accessed 24 April 2021.

[66] 'The Online Regulation Series | The European Union' (*tech against terrorism*, 19 October 2020) <www.tech againstterrorism.org/2020/10/19/the-online-regulation-series-the-european-union/> accessed 24 April 2021.

[67] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L 124/36.

[68] Regulation 2021/784, Recital 45.

[69] Directive (EU) 2017/541.

[70] 'EU online terrorist content legislation risks undermining press freedom, (*Committee to Protect Journalists*, 11 March 2020) <https://cpj.org/2020/03/eu-online-terrorist-content-legislation-press-freedom/> accessed 23 April 2021.

for the infringement of this Regulation do not encourage the removal of material which is not terrorist content'.[71]

Furthermore, another concern arises as a consequence of this key element. According to the Regulation any assigned competent authority will have the power to order the deletion of online content, hosted anywhere in the EU.[72] This means that one member state can extend its enforcement jurisdiction beyond its territory without prior judicial review and consideration for the rights of individuals in the affected jurisdictions.[73]

In light of the serious threats to the rule of law in certain EU Member States, the mutual trust that underpins the European judicial cooperation might be undermined. Furthermore, the procedure of minimal notification to and verification by the affected state foreseen in the current text seems not to contain sufficient safeguards against state overreach and possible abuse of power.[74] In addition, due to the short one-hour time limit, online platforms may have the perception that there is no other option but to comply with the removal orders to avoid fines or legal problems disregarding the few safeguards that are put into place. Moreover, the regulation does not solve disagreements among the EU countries over what constitutes as terrorism, irony, art, or journalistic reporting.[75] Consequently, different perceptions of the concepts can lead to problematic situations.

This could open the way for authoritarian regimes, like those in Poland and Hungary, to silence their critics abroad by issuing removal orders beyond their borders. This way, they can effectively extend their jurisdiction beyond their borders.[76] For example, Germany could be subject to removal orders from Hungary. As Patrick Breyer[77] pointed out: '[t]he fact that Victor Orbán will be able to have digital content deleted throughout the EU opens the door to politically motivated internet censorship – especially since the definition of terrorism is alarmingly broad and susceptible to abuse.'

Moreover, because of the broad definition of 'terrorist content' as mentioned above, there is a possibility that orders for political purposes may be issued in the name of fighting terrorism. Whether national standards will consequently be precluded is a different question. Worth noting is that the regulations relating to video sharing platforms were

---

[71] Regulation 2021/784, recital 45.

[72] Regulation (EU) 2021/784.

[73] 'Free Speech Advocates Urge EU Legislators to Vote 'No' to Automated Censorship Online' (*Liberties*, 25 March 2021) <www.liberties.eu/en/stories/terrorist-content-regulation-open-letter-to-meps/43410> accessed 24 April 2021.

[74] Ibid.

[75] Patrick Breyer, 'Controversial EU anti-terror internet regulation terreg adopted: freedom of expression and press in danger' (*Patrick Breyer*, 12 January 2021) <www.patrick-breyer.de/en/controversial-eu-anti-terror-internet-regulation-terreg-adopted-freedom-of-expression-and-press-in-danger/?lang=en> accessed 24 April 2021.

[76] Ibid.

[77] Patrick Breyer is a Committee Member (European Pirate Party) who participated in the negotiations as the Greens/EFA group's shadow rapporteur.

initially intended to achieve maximum harmonisation but were reduced to minimal harmonisation as a result of Council amendments (the Council amendments also introduced provisions on terrorist content based on the same definition).[78]

The problem with a broad definition is also noticeable with anti-terror laws that have repeatedly been used for completely different purposes in the European Union countries. Some examples include anti-terror laws against the Catalan independence movement, against social protests in France, against climate activists and against immigrants.[79]

6 Regulation Applied to the Web

6.1 Defining the Web

The Surface Web, which is among others also called the Visible Web and Indexed Web, is the portion of the World Wide Web that is readily available to the general public. It can easily be accessed with standard web search engines such as Google.[80] Furthermore, the Surface Web is also referred to as the 'upper' layer of the Web. The 'deeper' layers, the content of the Deep Web, are not indexed by traditional search engines such as Google. If we go even deeper, in the deepest layers of the Deep Web, there is a third category that is called the 'Dark Web'. This third category contains content that has been intentionally concealed.[81] The Dark Web can only be accessed through specialized browsers.[82] This paper only examines the applicability of the regulation to the Surface Web. Nonetheless, the regulation as it currently stands provides the option for competent authorities to become active on both the Deep Web and the Dark Web. The regulation requires that the content must be made public and entails some form of service. The definition on the public states that content should be made available to a 'potentially unlimited number of persons'. This might seem restrictive. However, considering the Dark Web, a person actually only needs a particular software and is able to access the dark web. On top of that, the service concept does not impose any limitation, as the service should only 'normally provided for remuneration', even if a person does not pay with financial means for the service; payment can be made in various forms. In this manner, the Regulation is opened to the Deep Web and the Dark Web.

[78] Lorna Woods, 'Crushing terrorism online – or curtailing free speech? The proposed EU Regulation on online terrorist content' *(EU Law Analysis,* 21 September 2018) <http://eulawanalysis.blogspot.com/2018/09/crushing-terrorism-online-or-curtailing.html> accessed 6 September 2021.

[79] European Pirate Party, 'Controversial EU anti-terror internet regulation terreg adopted: freedom of expression and press in danger' (*European Pirate Party,* 13 January 2021) <https://european-pirate-party.eu/controversial-eu-anti-terror-internet-regulation-terreg-adopted-freedom-of-expression-and-press-in-danger/> accessed 24 April 2021.

[80] Gabriel Weimann, 'Terrorist Migration to the Dark Web' [2016] 3(10) JSTOR, 40.

[81] Ibid.

[82] Ibid.

6.2 Applicability of the Regulation

The rules of the Regulation apply to hosting service providers offering services in the EU whether or not they have their main establishment in the member states.[83] This is an important point in the Regulation, as terrorist content is not only disseminated through services provided by hosting service providers in the EU. Recital 15 states that the hosting service providers are often established in third countries. Therefore, the Regulation applies to all providers offering relevant services in the European Union, irrespective of their main establishment.[84] This way, the Regulation tries to protect users in the EU and ensure that all hosting service providers operating in the digital single market have to comply to the same requirements.[85] Further, the Regulation also defines 'offering services' in the EU, ie if the services enable natural or legal persons to use its services in at least one member state. Moreover, also if it has a substantial connection to at least one member state.[86]

The Regulation only applies to providers of information society services which store and disseminate information and material to the public.[87] It does not matter whether the storing is of a mere technical, automatic and passive nature. The concept of 'storage' refers to holding data in the memory of a physical or virtual server. Consequently, the following providers fall outside the scope of this Regulation: 'providers of "mere conduit" or "caching" services, as well as of other services provided in other layers of the internet infrastructure, which do not involve storage, such as registries and registrars, as well as providers of domain name systems (DNS), payment or distributed denial of service (DdoS) protection services'.[88] Regarding the Proposed Regulation, there were numerous critiques to be heard in view of the fact that no difference was made between the application level and the infrastructure level that could lead to disproportionate interferences.[89] The Regulation has made some necessary adaptions to ensure differentiaton between both levels. However, there is still a wide scope, as layers on the internet infrastructure level where storage is involved still fall inside the scope of this Regulation.

Interpersonal communication services, as defined in point (5) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council[90], such as emails or private messaging services, fall outside the scope of this Regulation. Further, providers of services, such as cloud infrastructure, which are provided at the request of parties other

[83] Council, 'Terrorist content online: Council adopts new rules'.
[84] Regulation 2021/784, Recital 15.
[85] ibid.
[86] Ibid.
[87] Regulation 2021/784, recital 26.
[88] Ibid.
[89] Aleksandra Kuczerawy, 'The proposed Regulation on preventing the dissemination of terrorist content online: safeguards and risks for freedom of expression' (2018) Center for Democracy and Technology < The Proposed Regulation on Preventing the Dissemination of Terrorist Content Online: Safeguards and Risks for Freedom of Expression by Aleksandra Kuczerawy :: SSRN> accessed 24 April 2021.
[90] European Parliament and Council Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36.

than the content providers and only indirectly benefit the latter, should not be covered by this Regulation.[91]

According to Recital 14, the Regulation covers, for example, providers of social media, video, image and audio-sharing services, as well as file-sharing services and other cloud services, insofar as those services are used to make the stored information available to the public at the direct request of the content provider.[92] A question that comes to mind when analysing the applicability of the Regulation is what to do with private messaging services such as WhatsApp that, as stated above, do not fall inside the scope of this Regulation. Nevertheless, these messaging services contain sometimes groups of people that talk and share terrorist content. On the one hand, we can interpret it as dissemination to the public, however, on the other, it is also private messaging between people. There are still some unclarities about the applicability on the Surface Web. In the following section, a case is being analysed in order to cite some possible issues that may arise.

6.3 Case example: Islamic State on media platforms

6.3.1 Islamic State and Telegram

The applicability of the Regulation on the surface web is not infallible. The program of Extremism at the George Washington University has collected and analysed 636 English-language pro-IS channels and groups on Telegram from June 1, 2017, to October 24, 2018.[93] In their report: 'Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram', they share their findings.

Telegram is an online instant messaging service. The application is very popular among adherents of the Islamic State (IS). Moreover, it remains vital to the organization's ecosystem of communications.[94] It offers IS sympathizers a user-friendly medium. The platform has functional affordances and a relatively lax enforcement of Telegram's terms of service (ToS).[95] They exploit Telegram's suite of features to communicate with like-minded supporters across the world, disseminate official and unofficial IS media, and provide instructional material for operations.[96] Nevertheless, IS is very critical about Telegram. The users said, as sometimes stated in a few cases, that it is best not to use it due to lack of security. However, it is the only platform that is still very popular among IS members because of its security.[97]

---

[91] Regulation 2021/784, recital 14.

[92] Ibid.

[93] Bennett Clifford and Helen Powell, 'Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram', Program on Extremism – The George Washington University <Encrypted Extremism Inside the English-Speaking Islamic State Ecosystem on Telegram - The George ... (readkong.com)> accessed 24 April 2021.

[94] Ibid.

[95] Ibid.

[96] Ibid.

[97] Ibid.

Government responses to terrorist exploitation of Telegram have been largely disincentive-based. Platforms who fail to moderate terrorist content are threatened with fines or bans.[98] The Regulation follows the same route by putting penalties in place when the platforms do not successfully engage in removing the content within the requested time after a removal order is send out.[99] Pressuring companies into taking tougher stances, provided that the company would avoid economic or legal issues by complying, could be effective in most cases. Nevertheless, Telegram, as a multinational, data-distributed, shareholder-free entity, would not be affected by many of the disincentives that governments attempt to apply to social media providers.[100]

It would be advised to also take an alternative approach, for example, by encouraging Telegram to participate in industry-led mechanisms for cooperation between technology companies. The Regulation should not abandon disincentives in cases of non-compliance. However, they can encourage the service provider to employ best practices developed through industry-led, not government-mandated, forums.[101] This could stimulate knowledge-sharing between Telegram and other platforms. Furthermore, it could improve their collective capacity for effective content moderation. Through knowledge-sharing they could prevent IS content on Telegram to shift onto the public-facing web through file-sharing or smaller social media platforms.[102]

6.3.2 Islamic State on small platforms

Furthermore, the Islamic State is currently experimenting with new smaller platforms to share their propaganda.[103] 'Following the key conclusions of the European Counter Terrorism Centre's (ECTC) Advisory Network Conference at Europol, experts agree that terrorist groups carefully assess platforms and choose to settle on those that offer maximum' security, stability, usability, and audience reach.[104] Firstly, they find it important to have high-security standards to increase operational security. Secondly, they want to know to what extent IS media operators and supporters are protected from any interferences by the platform owner and/or third parties. In this regard, they refer to, for example, content and account removals. Thirdly, the app should be easily usable on a daily basis. Finally, they want to reach as many users as they can, even if the platforms are rather small.[105]

---

[98] Ibid.

[99] Regulation 2021/784, Article 18.

[100] B. Clifford and H. Powell, 'Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram', *Program on Extremism*, June 2019, 1 - 55 p.

[101] Ibid.

[102] Ibid.

[103] 'Analysis: ISIS use of smaller platforms and the DWeb to share terrorist content' (*tech against terrorism*, 29 April 2019*)* <www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019/> accessed 24 April 2021.

[104] Ibid.

[105] Ibid.

Bigger social media platforms such as Twitter and YouTube have the resources to combat the dissemination of terrorist content. Nevertheless, smaller platforms may not have the required resources to tackle the problem which may lead to shifting the problem.[106] It will be important to keep an eye on the smaller platforms and see if they also are able to fulfil their part in ending the dissemination of terrorist content online. If not, alternative approaches or (less expensive) tools should be identified to find a solution to this problem.

7 Conclusion

Considering the main scope, that being the concept of 'terrorist content', the Regulation underwent changes throughout the legislative process. This happened under the influence of several international and European actors. The wording of the scope was amended, but unclarity is still part of the core elements of the definition of 'terrorist content'.

Amendments have been made throughout the entire Regulation. EDRi still had multiple concerns and urged the Members of the European Parliament to vote against the adoption of the regulation, but their efforts failed. One of their concerns was the competent authorities' lack of independence. It is impossible to argue that these authorities should be independent, not only based upon the wording of the regulation but also regarding other fundamental rights which should be assessed by independent authorities. The lack of these independent authorities could be harmful for the fundamental rights of all EU citizens and the EU itself. Not only would it be possible that certain rights would disproportionally be affected, additionally, it could harm the EU, as mutual trust which underpins European criminal cooperation would face troubles since the authorities could order or decide to remove terrorist content for political reasons due to outside pressure. To prevent issues of mutual trust in the longer term, the competent authorities should be independent. Aside from this, a currently lacking cooperation mechanism in the form of a group bringing together the different competent authorities should be established.

Furthermore, two key elements were identified that come along with the Regulation. First, the Regulation encourages Member States to take 'proactive measures', such as automated tools, to prevent terrorist content from being uploaded. More specifically, the regulation states that the hosting service provider should provide appropriate technical and operational measures or capacities.[107] Nevertheless, some companies are not willing to devote unlimited resources to terrorist content. Consequently, there may be a chance that they are going to use 'technical means', such as machine learning algorithms and

[106] Ibid.
[107] Regulation 2021/784, Article 5(2).

upload filters. According to the Commission's Impact Assessment tools are still immature and therefore require human verification.[108]

It is sometimes impossible for automation to differentiate between parody, satire, educational material and actual terrorist content. The Regulation has put in place some requirements that need to be fulfilled in order to prevent a negative outcome of these automated tools. However, these safeguards seem not to be enough in order to avoid these errors, as the Regulation relies on AI developers to implement technical solutions to complex social issues.

Another key element of the Regulation entails that Member States will be able to issue swift removals across borders. They will be obliged to remove content or disable access within one hour of having received a removal order from a competent authority, appointed by the Member Sate. In this paper, a few concerns regarding this key element were addressed. The one-hour deadline and fear of financial penalties can result in removing content that is shared for journalistic and academic purposes and thus not terrorist content,[109] limiting our ability to obtain information and express ourselves freely.

In addition, any assigned competent authority will have the power to order the deletion of online content hosted anywhere in the EU.[110] Nevertheless, the Regulation does not solve disagreements among the EU countries over what constitutes as terrorism, irony, art, or journalistic reporting.[111] The procedure of minimal notification to and verification by the affected state foreseen in the current text seems to not contain sufficient safeguards against state overreach and possible abuse of power. [112]

Moreover, the Regulation has been analysed on its applicability to the Surface Web with a case example. Through this example, it was noted that the applicability of the Regulation on the Surface Web is not infallible. Multinational, data-distributed, shareholder-free entities are most likely not to be affected by many of the disincentives that the Regulation applies to providers. Instead, an alternative approach can be taken, for example, through knowledge-sharing between platforms such as Telegram and others.[113] The sharing of best practices can improve the collective capacity for effective content moderation.

---

[108] Commission, 'Staff Working Document Impact Assessment Accompanying the document Porposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online', SWD(2018) 408 final.

[109] 'EU online terrorist content legislation risks undermining press freedom, (*Committee to Protect Journalists,* 11 March 2020) <https://cpj.org/2020/03/eu-online-terrorist-content-legislation-press-freedom/> accessed 23 April 2021.

[110] Regulation (EU) 2021 of the European Parliament and the Council of 18 March 2021 on addressing the dissemination of terrorist content online.

[111]Patrick Breyer, 'Controversial EU anti-terror internet regulation terreg adopted: freedom of expression and press in danger' (*Patrick Breyer,* 12 January 2021) <www.patrick-breyer.de/en/controversial-eu-anti-terror-internet-regulation-terreg-adopted-freedom-of-expression-and-press-in-danger/?lang=en> accessed 24 April 2021.

[112] Ibid.

[113] Ibid.

Furthermore, it will be important to keep an eye on the smaller platforms and see if they are also able to fulfil their part in ending the dissemination of terrorist content online since smaller platforms may not have the required resources to tackle the problem, which may lead to shifting the problem.

References

'Analysis: ISIS use of smaller platforms and the DWeb to share terrorist content' (tech against terrorism, 29 April 2019) <www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019/> accessed 24 April 2021.

'EU online terrorist content legislation risks undermining press freedom, (Committee to Protect Journalists, 11 March 2020) <https://cpj.org/2020/03/eu-online-terrorist-content-legislation-press-freedom/> accessed 23 April 2021.

'European Union: independent judiciary and effective remedies must be at the core of the EU Regulation on "Terrorist Content Online", warns ICJ' (International Commission of Jursits, 7 December 2020) <European Union: independent judiciary and effective remedies must be at the core of the EU Regulation on "Terrorist Content Online", warns ICJ | International Commission of Jurists> accessed 24 April 2021.

'Free Speech Advocates Urge EU Legislators to Vote 'No' to Automated Censorship Online' (Liberties, 25 March 2021) <www.liberties.eu/en/stories/terrorist-content-regulation-open-letter-to-meps/43410> accessed 24 April 2021.

'Open latter: Civil society urges Member States to respect the principles of the law in Terrorist Content Online Regulation' (EDRI, 27 March 2020) <https://edri.org/our-work/open-letter-civil-society-urges-member-states-to-respect-the-principles-of-the-law-in-terrorist-content-online-regulation/> accessed 27 April 2021.

'The Online Regulation Series | The European Union' (tech against terrorism, 19 October 2020) <www.techagainstterrorism.org/2020/10/19/the-online-regulation-series-the-european-union/> accessed 24 April 2021.

Breyer P, 'Controversial EU anti-terror internet regulation terreg adopted: freedom of expression and press in danger' (Patrick Breyer, 12 January 2021) <www.patrick-breyer.de/en/controversial-eu-anti-terror-internet-regulation-terreg-adopted-freedom-of-expression-and-press-in-danger/?lang=en> accessed 24 April 2021.

Clifford B and Powell H, 'Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram', Program on Extremism – The George Washington University <Encrypted Extremism Inside the English-Speaking Islamic State Ecosystem on Telegram - The George ... (readkong.com)> accessed 24 April 2021.

EDRi, 'All Cops Are Blind? Context in terrorist content online' (EDRI, 13 February 2019) <All Cops Are Blind? Context in terrorist content online - European Digital Rights (EDRi)> accessed 24 April 2021.

EDRi, 'EDRi Amendments on the proposal for a Regulation to prevent the dissemination of terrorist content online' (2019) < 20190116_EDRi_ProposalForAms.pdf> accessed 24 April 2021.

EDRi, 'EU's AI proposal must go further to prevent surveillance and discrimination' (EDRi, 21 April 2021) <https://edri.org/our-work/eus-ai-proposal-must-go-further-to-prevent-surveillance-and-discrimination > accessed 24 April 2021.

European Pirate Party, 'Controversial EU anti-terror internet regulation terreg adopted: freedom of expression and press in danger' (European Pirate Party, 13 January 2021) <https://european-pirateparty.eu/controversial-eu-anti-terror-internet-regulation-ter-reg-adopted-freedom-of-expression-and-press-in-danger/> accessed 24 April 2021.

Kayyali D, 'It's not too late for Members of European Parliament to vote no on the disastrous "Terrorist content" regulation' (MNEMONIC, 25 March 2021) <https://mnemonic.org/en/content-moderation/Mnemonic-joins-61-organisations-urging-EU-to-vote-no> accessed 23 April 2020.

Kuczerawy A, 'The proposed Regulation on preventing the dissemination of terrorist content online: safeguards and risks for freedom of expression' (2018) Center for Democracy and Technology < https://cdt.org/insights/research-paper-from-leuven-university-proposed-regulation-on-preventing-the-dissemination-of-terrorist-content-online/> accessed 24 April 2021.

Special Rapporteur David Kaye, Special Rapporteur Joseph Cannataci and Fionnuala Ni Aoláin, 'Com-ments on the Proposal for a Regulation on preventing the dissemination of terrorist content online to complement Directive 2017/541 on combating terrorism' (7 December 2018) OL OTH 71/2018.

Walker K, 'Four steps we're taking today to fight terrorism online' (Blog Google, 18 June 2017) <www.blog.google/topics/google-europe/four-steps-were-taking-today-fight-online-terror/> accessed 24 April 2021.

Weimann G, 'Terrorist Migration to the Dark Web' [2016] 3(10) JSTOR, 40.

Woods L, 'Crushing terrorism online – or curtailing free speech? The proposed EU Regulation on online terrorist content' (EU Law Analysis, 21 September 2018) <http://eulawanalysis.blogspot.com/2018/09/crushing-terrorism-online-or-curtailing.html> accessed 6 September 2021.

Until the end of the 1990s, EU integration in the area of criminal law centred primarily around the regional deepening of traditional judicial cooperation in criminal matters and the development of law enforcement cooperation (including the setting up of Europol as a support agency). By the end of the 1990s respectively 2000s, the EU also gained (limited) supranational competence in the areas of substantive respectively procedural criminal law. Both judicial and law enforcement cooperation were furthered over the years via the principles of mutual recognition respectively availability, and through the setting up (and development) of Eurojust, the establishment of a European Public Prosecutor's Office and the further development of Europol. After three decennia, the EU criminal law corpus is impressive – a core component of the EU's 'Area of Freedom, Security and Justice', building on and adding to (both real and presumed) trust between the Member States.

No time for stand-still, though. Since 2020, the European Commission has launched a tsunami of new legislative proposals, including in the sphere of EU criminal law, strongly framed in its new EU Security Union Strategy.

This special issue on 'EU criminal policy. Advances and challenges' discusses and assesses some of the newest developments, both in an overarching fashion and in focused papers, relating to key 2022 novelties for Europol (ie the competence to conduct AI-based pre-analysis in (big) data sets, and extended cooperation with private parties), the sensitive debate since 2020 on criminalising (LGBTIQ) hate speech and hate crime at EU level, the 2022 Cybersecurity Directive, the potential of the 2020 Conditionality Regulation to address rule of law issues undermining the trustworthiness of Member States when issuing European Arrest Warrants, and concerns about free speech limitation by the 2021 Terrorist Content Online Regulation.

Gert Vermeulen is Senior Full Professor of European and international Criminal Law and Data Protection Law, Director of the Institute for International Research on Criminal Policy (IRCP), of the Knowledge and Research Platform on Privacy, Information Exchange, Law Enforcement and Surveillance (PIXLES) and of the Smart Solutions for Secure Societies (i4S) business development center, all at Ghent University, Belgium. He is also General Director Publications of the AIDP and Editor-in-Chief of the RIDP.

Wannes Bellaert is PhD Researcher and Academic Assistant at the Institute for International Research on Criminal Policy (IRCP), Ghent University.

www.maklu.be
ISBN 978-90-466-1134-0