Public Provocation to Commit a Terrorist Offence: Balancing Between the Liberties and the Security* 

by 

Kristina Ramešová **

Modern terrorism is global and decentralized like cyberspace. While the Darknet is mostly used by terrorists for fundraising campaigns and illicit trading, publicly accessible social platforms such as Twitter, Facebook or YouTube are abused for terrorist propaganda. Combating terrorism remains one of the top priorities of the European Union (hereinafter as “the EU”). The approach towards the online content possibly connected to terrorist propaganda has become stricter.

This paper focuses on the development of the EU legislation on the offence related to terrorist activities: the public provocation to commit a terrorist offence, as well as on the obligations of hosting service providers. It also analyses the impact of the Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. The article observes a changing attitude on private monitoring of online information in the development of the EU legislation. It analyses changes in the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online. These changes signify a shift in the perception of the necessary level of freedom to receive and impart information through the internet.

* The article has been supported under the grant No. SVV 260 359 financed by the Faculty of Law, Charles University.

** kristina.ramesova@email.cz, Ph.D. Candidate at the Department of Administrative Law and Administrative Science, Faculty of Law, Charles University, The Czech Republic.
KEY WORDS
Dissemination of Terrorist Content Online, Hosting Service Providers, Provocation to Commit a Terrorist Offence, Terrorism

1. INTRODUCTION
Social media have become an important part of everyday life. About 95% of all information on the planet is digital, most of it is accessible via computer networks.1 Approximately 3 billion people have accounts on Facebook, Instagram, Messenger and (or) WhatsApp.2

A general agreement on a universal legal definition of terrorism does not exist.3 Numerous international treaties and declarations use their own definitions. The Arab Convention for the Suppression of Terrorism defines terrorist acts as:

“any act or threat of violence, whatever its motives or purposes, that occurs in the advancement of an individual or collective criminal agenda and seeking to sow panic among people, causing fear by harming them, or placing their lives, liberty or security in danger, or seeking to cause damage to the environment or to public or private installations or property or to occupying or seizing them, or seeking to jeopardise a national resource.”4

The Council of Europe Convention on the Prevention of Terrorism defines a terrorist offence as “any of the offences within the scope of and as defined in one of the treaties listed in the Appendix” of the aforementioned convention.5 Regardless of numerous sector specific international treaties and definitions of terrorism, the Special Tribunal for Lebanon has ruled on the basis

---

1 Hilbert, M. and López, P. (2011) The World’s Technological Capacity to Store, Communicate, and Compute Information. Science, 332 (6025), pp. 60–65. Available from: http://science.sciencemag.org/content/332/6025/60 [Accessed 16 May 2020].
2 Facebook. (2020) Facebook Q1 2020 Results. Investor Relations. [online] Available from: https://s21.q4cdn.com/399680738/files/doc_financials/2020/q1/Q1-2020-FB-Earnings-Presentation.pdf [Accessed 16 May 2020].
3 Sanyal, S. (2015) International Laws to Control Terrorism: A Comparative Study. AAKROSH Asian Journal on Terrorism and Internal Conflicts, p.3. Available from: http://dx.doi.org/10.2139/ssrn.3232739 [Accessed 16 May 2020].
4 Art. 1(2) Arab Convention for the Suppression of Terrorism. Adopted by the Council of Arab Ministers of the Interior and the Council of Arab Ministers of Justice, 22 April 1998. Available from: https://www.unodc.org/images/tldb-f/conv_arab_terrorism.en.pdf [Accessed 16 May 2020].
5 Art. 1(1) Council of Europe Convention on the Prevention of Terrorism, 16 May 2005. Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808c3f55 [Accessed 16 May 2020].
of treaties, *United Nations* resolutions and the legislative and judicial practice of States: There is a customary rule of international law regarding the international crime of terrorism in time of peace,\(^6\) pursuant to which terrorism requires the following three key elements: (i) the intent (*dolus*) of the underlying crime and (ii) the special intent (*dolus specialis*) to spread fear or coerce authority; (iii) the commission of a criminal act, and (iv) that the terrorist act be transnational.\(^7\)

The EU is facing a range of terrorists attacks both from networked groups and lone actors.\(^8\) Cyberspace\(^9\) enables terrorists to find a suitable target and to lead an attack almost from anywhere.\(^{10}\) According to *Europol*, religiously motivated terrorist groups use the internet and social media to gain instruments of crime and to share information secretly via electronic services as *WhatsApp*, *Viber* or *Skype*; social platforms as *Facebook* and *Twitter* have been used for propaganda, recruitment or sharing information inside closed groups.\(^{11}\) The EU is aware of growing threat of terrorism and the abuse of cyberspace, particularly the use of internet for propaganda, recruitment, effective communication, planning etc. Combating terrorism remains one of the top priorities of the EU.\(^{12}\)

According to *Europol*:

"[a]s the line between online and offline communities becomes increasingly blurred, terrorist propaganda preying on human suffering abroad reaches

---

\(^6\) Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging. (2011) STL-11-01/1, Special Tribunal for Lebanon, 16 February 2011. Available from: https://www.refworld.org/cases,STL,4d6280162.html [Accessed 16 May 2020].

\(^7\) Op. cit., para. 85.

\(^8\) *EUROPOL*. (2019) The European Union Terrorism Situation and Trend Report 2019. Available from: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat [Accessed 16 May 2020].

\(^9\) Virtual environment of interconnected computer devices and networks, i.e. space enabling sharing information and mutual communication. See Barlow, J. P. (1990) Crime and Puzzlement: in advance of the law on the electronic frontier. *Whole Earth Review*, pp. 44–57.

\(^10\) *EUROPOL*. (2016) Changes in Modus Operandi of Islamic State (IS) Revisited. Available from: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited [Accessed 16 May 2019]; United Nations. (2019) New technologies, artificial intelligence aid fight against global terrorism. [press release] September 4. Available from: https://news.un.org/en/story/2019/09/1045562 [Accessed 16 May 2020].

\(^11\) Op. cit., pp. 4, 11–12; *EUROPOL*. (2019) Internet Organised Crime Threat Assessment (IOCTA), p. 48. Available from: https://www.europol.europa.eu/iocta-report [Accessed 16 May 2020].

\(^12\) European Council. (2018) EU Counter-Terrorism Strategy. Available from: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/eu-strategy/ [Accessed 16 May 2020].
audiences in Europe to unprecedented extents, inciting some to act and driving others to embrace extremist views on the opposite end.”

Furthermore:

“IS succeeded in maintaining an online presence largely thanks to unofficial supporter networks and pro-IS media outlets. Pro-IS and pro-al-Qaeda channels promoted the use of alternative platforms and open source technologies.”

Terrorist groups continue to exploit a wide array of online service providers, including forums, file sharing sites, video streaming and sharing sites, blogs, messaging and broadcast applications, social media sites etc. Social platform propaganda is powerful: the stronger and the more vivid the online content is, the more it is going to be perceived as likely to occur in the future, even if not experienced personally.

Understandably, the EU approach towards online content possibly connected to terrorist propaganda has become stricter. Claiming to ensure a smooth functioning of the Digital market, the European Commission (hereinafter as “the Commission”) presented a draft of a new regulation on 12 September 2018: the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (hereinafter as “the proposal of online terrorist content regulation” or “the Proposal”), which has been introduced at the end of transposition period of the Directive 2017/541/EU on combating terrorism (hereinafter as “the Counter-Terrorism directive”) on 8 September 2018.

---

13 EUROPOL. (2019) The European Union Terrorism Situation and Trend Report 2019, p. 5. Available from: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat [Accessed 16 May 2020].
14 Islamic State, hereinafter as “IS”.
15 Op. cit., p. 7.
16 EUROPOL. (2019) Internet Organised Crime Threat Assessment (IOCTA) 2019, p. 48. Available from: https://www.europol.europa.eu/iocta-report [Accessed 16 May 2020].
17 Plous, S. (1993) The Psychology of Judgement and Decision Making. New York: McGraw-Hill, p. 126.
18 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].
19 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. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].
The transposition has not yet been completed in all the EU member states.\textsuperscript{20} Also, the Commission’s report assessing the extent to which member states have taken measures to comply with the Counter-Terrorism directive and the report assessing its added value, were both not submitted yet.\textsuperscript{21}

This paper aims to analyse the development of the EU legislation regarding an offence related to terrorist activities which could be easily perpetrated online: public provocation to commit a terrorist offence. The focus is put on the legislation. As the danger consists of targeting different audiences, worldwide accessibility and possible influence on wide international public opinion,\textsuperscript{22} the phenomenon is currently used in the process of advocating new legislative endeavours concerning the prevention of disseminating terrorist content online.\textsuperscript{23}

The definition of public provocation to commit a terrorist offence has been clarified in the Counter-Terrorism directive, which also regulates provisions regarding criminal liability, imposes an obligation to criminalise aiding and abetting, inciting and attempting, and determines the possibility for criminal liability of legal persons.\textsuperscript{24} However, it seems the measures set up in the Counter-Terrorism directive are not sufficient. Another legislation that shall be directly applicable in all the EU member states has been proposed. Therefore, following questions arise: what is the Counter-Terrorism directive’s legal regulation of public provocation to commit a terrorist offence? What changes are suggested by the proposal of online terrorist content regulation and why? What do these changes signify?

\textsuperscript{20} Greece, Cyprus and Luxembourg did not comply with the transposition before the deadline. See National transposition measures communicated by the Member States concerning: 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. Available from: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32017L0541 [Accessed 16 May 2020].

\textsuperscript{21} According to Art. 29 of the Counter-Terrorism directive, reports shall be given to the European Parliament and to the Council by 8 March 2020 and 8 September 2021.

\textsuperscript{22} Broadhurst, R. et al. (2017) Cyber terrorism: research report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology, p. 67. Available from: https://ssrn.com/abstract=2984101 or http://dx.doi.org/10.2139/ssrn.2984101 [Accessed 16 May 2020].

\textsuperscript{23} Proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/0640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

\textsuperscript{24} Art. 5, 13–14, 17–18 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. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861 &uri=CELEX:32017L0541 [Accessed 16 May 2020].
A short insight to the development of legislation on terrorism and terrorist offences in the EU and an analysis of the term “public provocation to commit a terrorist offence” are presented. The wording of the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, amended by the Decision 2008/919/JHA (hereinafter as “Framework Decision 2008”) is compared with the Counter-Terrorism directive. The objectives of the legislation are emphasized and problematic parts in the Counter-Terrorism directive’s interpretation are pointed out. The definition of public provocation to commit a terrorist offence is compared with the terrorist content definition presented in the proposal of online terrorist content regulation.

2. DEVELOPMENT OF LEGISLATION AND HARMONISATION OF TERRORIST OFFENCES IN THE EU

The EU started harmonising definitions of terrorist offences in the member states’ legislation after terrorist attacks on the World Trade Centre on 11 September 2001. Along with the Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism, definitions of eleven terrorist acts were adopted. Until recently the cornerstone of criminal response to counter terrorism had been the Framework Decision 2008 which has defined a “public provocation to commit a terrorist offence” for the first time as:

“the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the offences listed in Article 1(1)(a) to (h), where such conduct, whether or not directly

---

25 Council Framework Decision of 13 June 2002 on combating terrorism and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. Official Journal of the European Union. Consolidated version Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002F0475-20081209 [Accessed 16 May 2020].

26 According to Art. 3 of the Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism, for an act to be considered a terrorist act, there have to be (1) intention, (2) serious damage for a country or an international organisation, (3) being the offence under national law, and (4) presence of at least one of three particularly stipulated motives.

27 Council Framework Decision of 13 June 2002 on combating terrorism and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. Official Journal of the European Union. Consolidated version Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002F0475-20081209 [Accessed 16 May 2020].
advocating terrorist offences, causes a danger that one or more such offences may be committed.”

After the adoption of the Framework Decision 2008, most of the EU member states introduced measures criminalising public provocation to commit a terrorist offence. According to the Commission’s report from 2014, less than half of the EU member states had adopted specific provisions explicitly criminalising the dissemination of messages to the public:

“with a view to inciting terrorist offences, closely aligned to the wording of the Framework Decision 2008”.

However, many of the member states remained on a general level, i.e. criminalising incitement, provocation, facilitation and support of terrorist offences. Different terms used in national legislations left some room for interpretation. According to the Commission, relying on more general terms, instead of relying on the mere intent to incite terrorist offences, might lead to the risk that only “direct provocation” not also “indirect provocation” would be criminalised. Regarding the incitement to terrorism, national courts have opposed broad definitions in favour of narrow interpretation in order to avoid restricting the freedom of expression and comply with the Article 10 of the European Convention on Human Rights. The Framework Decision 2008 did not satisfactorily answer questions on where the free speech ends and the incitement begins. Demands on defining limits between public provocation to commit a terrorist offence and the freedom of speech in a clearer way persisted and

28 Op. cit., Art. 3 (1) (a).
29 European Commission. (2008) The Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism, p. 5. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52014DC0554 [Accessed 16 May 2020].
30 In 2014 the provisions were explicitly limited to the direct provocation in Belgium, France and Estonia. A risk of not criminalising the indirect provocation existed in Italy, Hungary, Malta and Lithuania. See op. cit., p. 6.
31 In 2007, when ruling in the case of a Basque punk band accused for a song referencing the Guardia Civil as the targets of ETA, a Basque separatist organisation, the Spanish Supreme Court ruled that a narrow interpretation of the incitement provision in Spanish criminal code is needed in order to comply with the Article 10 of the ECHR. Rediker, E. (2015) The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union. Michigan Journal of International Law, 36 (2), pp. 338–342. Available from: https://repository.law.umich.edu/mjil/vol36/iss2/3/ [Accessed 16 May 2020].
proposals to replace old framework decisions with a new directive appeared.\textsuperscript{32}

On 12 December 2015 the Commission proposed a draft of the new Counter-Terrorism directive. The draft aimed not only to adapt the EU legislation to the dissemination of messages, images and other material related to terrorism online, but also to clarify what shall be considered as terrorist offences in the EU. On 15 March 2017 the EU adopted the Counter-Terrorism directive in order to harmonise legislation on fighting terrorism and to adapt legal norms to specific transnational nature. The Counter-Terrorism directive replaced the Framework Decision 2008 and amended parts of the Decision 2005/671/JHA on sharing information and on the cooperation concerning terrorist offences. Regarding online social media, the Counter-Terrorism directive aims particularly to address online propaganda,\textsuperscript{33} recruitment,\textsuperscript{34} and other auxiliary behaviour,\textsuperscript{35} all of which increase the risk that terrorist offence would be committed.\textsuperscript{36}

3. OFFENCES WITHIN THE GENERAL CONCEPT OF TERRORISM

The Counter-Terrorism directive’s strength consists in approximation of definitions of terrorist offences, offences related to a terrorist group, and offences related to terrorist activities in all the EU member states.\textsuperscript{37} Legal provisions of fight to counter terrorism have been strengthened by criminalisation of behaviour that is a preparatory phase of crime, such

\textsuperscript{32} Ibid.
\textsuperscript{33} Art. 5–6 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. \textit{Official Journal of the European Union}. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].
\textsuperscript{34} Op. cit., Art. 6.
\textsuperscript{35} Op. cit., Art. 7–12.
\textsuperscript{36} Shamieh, L. and Szenes, Z. (2015) The Propaganda of ISIS/DAESH through the Virtual Space. \textit{Defence Against Terrorism Revue}, 7 (1), p. 9. Available from: http://www.coedat.nato.int/publication/datr/volumes/datr10.pdf [Accessed 16 May 2020]. For simplified and unified model of radicalisation process see Hunter, R. and Heinke, D. H. (2011) Radicalization of Islamist Terrorists in the Western World. \textit{FBI Law Enforcement Bulletin}, 9 (80), pp. 25–31. Available from: https://leb.fbi.gov/articles/perspective/perspective-radicalization-of-islamist-terrorists-in-the-western-world [Accessed 16 May 2020].
\textsuperscript{37} With an exception of United Kingdom, Ireland and Denmark. Rec. 41–42 of the Counter-Terrorism directive.
as recruitment (Art. 6), providing training for terrorism (Art. 8) or travelling for the purpose of terrorism (Art. 9).

The Counter-Terrorism directive recognises three groups of offences: (i) terrorist offences, (ii) offences related to a terrorist group and (iii) offences related to terrorist activities. The list of terrorist offences is exhaustive and encompasses only intentional acts explicitly mentioned in Art. 3, defined as offences under national law and, given their nature or context, being able to seriously damage a country or an international organisation, and in the case they were committed with the terrorist intention.\(^{38}\) The notion of terrorist intention must apply to all the elements of crime. Outside these conditions a misuse of information and communications technology (hereinafter as “ICT”) for propaganda, recruitment or dissemination of training instructions with the intent to commit or to contribute to the commission of any terrorist offence could be considered as offence related to terrorist activities. The offences linked to terrorist activities fall within the scope of the general concept of terrorism.\(^{39}\)

3.1. PUBLIC PROVOCATION TO COMMIT A TERRORIST OFFENCE

Among offences related to terrorist activities a particular interest is put on the offence of public provocation to commit a terrorist offence, which shall comprise glorification or justification of terrorism or dissemination of messages or images in order to gain support for terrorist purposes.\(^{40}\)

Public provocation to commit a terrorist offence is defined as:

\[
\text{"the distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission of one of the offences listed in points (a) to (i) of Article 3(1), where such conduct, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby}\]

---

\(^{38}\) Art. 3 (2) 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. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

\(^{39}\) Judgement of 31 January 2017, Lounani, C-573/14, ECLEU:C:2017:71, para. 50–51.

\(^{40}\) Rec. 10 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. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].
causing a danger that one or more such offences may be committed, is punishable as a criminal offence when committed intentionally.”

The EU member states shall criminalise not only aiding and abetting but also inciting the offence. In comparison to the Framework Decision 2008 the criminalisation of involvement in public provocation to commit a terrorist offence has been extended to inciting.

It is apparent that the definition is broader than the previous one in the Framework Decision 2008. The Counter-Terrorism directive’s definition emphasizes that the distribution (or otherwise making available) of the message to the public may occur by any means, either online or offline. Also, it stipulates expressly that it is not important if such distribution advocates the commission of listed terrorist offences directly or indirectly, because the Commission was afraid that the indirect provocation would not be criminalised in all member states. Another extension of the definition presents the list of terrorist offences intended to be incited by the provocation. Art. 3 (1) i) of the Counter-Terrorism directive provides for a new terrorist offence of illegal system interference; a disposal of radiological weapons and development of radiological or nuclear weapons are added to the definition of terrorist offence.

The further change concerns a fault which is presented in the definition of the offence itself. The Counter-Terrorism directive’s definition of public provocation to commit a terrorist offence has emphasized the intent (“… is punishable as a criminal offence when committed intentionally”), whether

---

41 Op. cit., Art. 5.
42 Op. cit., Art. 14 (1) (2).
43 Art. 4 (2) Council Framework Decision of 13 June 2002 on combating terrorism and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. Official Journal of the European Union. Consolidated version Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002F0475-20081209 [Accessed 16 May 2020]; Art. 14 (2) 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. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].
44 See Chapter 1.
45 Art. 3 (1) i) 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. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].
46 Op. cit., Art. 3 (1) f).
47 Op. cit., Art. 5.
the Framework Decision 2008 mentioned the intent in another provision, when demanding criminalisation of expressly stipulated intentional acts, such as public provocation to commit a terrorist offence.\textsuperscript{48} In the definition of public provocation to commit a terrorist offence itself, the Framework Decision 2008 mentioned the intent only when stipulating “the intent to incite the commission of one of the offences listed in Article 1(1)(a) to (h).”\textsuperscript{49} Nevertheless, the interpretation of fault should stay the same as in the Framework Decision 2008: the Framework Decision 2008 has stipulated that the distribution or otherwise making available of a message to the public, has to be perpetrated with the intent to incite the commission of one of the listed offences.\textsuperscript{50} Such distribution could be hardly committed in negligence, i.e. with no intent, as a perpetrator necessarily had to act with the particular intent to incite the commission of at least one of the offences listed in Article 1(1)(a) to (h) of the Framework Decision 2008.\textsuperscript{51}

Regarding the body of crime, the Counter-Terrorism directive evidently does not distinguish between online and offline environment. For the criminal liability it is not important. Nevertheless, it underlines that such conduct should be punishable when it causes a danger that terrorists acts may be committed; such danger should be considered regarding the addressee of the message.\textsuperscript{52} As the online illegal content spreads easily and reaches disproportionately more audiences (addressees) as possible, committing crime online may be considered as an aggravating circumstance. On the other hand, a particularly injurious effect of the crime committed online is disputable, as the actual effect of online propaganda in individual radicalisation of a perpetrator is not so clear. According to Heinke, even though an ideological framing may happen individually through the internet, yet in most cases social contacts with peers are more important; radicalisation does not often happen only after observing

\begin{footnotes}
\item[48] Art. 3 (2) a) Council Framework Decision of 13 June 2002 on combating terrorism and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. Official Journal of the European Union. Consolidated version Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002F0475-20081209 [Accessed 16 May 2020].
\item[49] Op. cit., Art. 3 (1) a).
\item[50] Op. cit., Art. 3 (1).
\item[51] Ibid.
\item[52] Rec. 10 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. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].
\end{footnotes}
a terrorist propaganda video or reading online radicalising message but through closer social relationships in a radicalised community of peers. Consequently, the effect of any particular offence should be addressed and evaluated in each individual case.

Further amendment to the previous definition of public provocation to commit a terrorist offence set by the Framework Decision 2008, is the causality between a distribution of the message to the public and the danger that any terrorist offence may be committed: it is explicitly stated that the indirect provocation is sufficient. The aim was to harmonise national legislation so that the indirect provocation would be criminalised in all the EU member states without an exception. Nevertheless, the interpretation of indirect provocation by national courts may still vary; a preliminary question to the Court of Justice of the EU has not yet been asked. The danger that a terrorist offence would be actually committed, should be judged according to specific circumstances of the case, such as who the author and the addressee of the message were and in which context the act is committed.

The Counter-Terrorism directive particularly proclaims that any of its provisions cannot be interpreted as the reduction or restriction to the dissemination of information for scientific, academic or reporting purposes; furthermore:

“the expression of radical, polemic or controversial views in the public debate on sensitive political questions, falls outside the scope of this directive and, in particular, of the definition of public provocation to commit terrorist offences.”

53 Heinke, D. H. (2016) Countering Radicalisation and Recruitment of so-called Jihadists – Proscription of Radicalization Hubs. Defence Against Terrorism Revue, 8, p. 92.
54 The Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (COM/2014/554 final) Available from: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/crisis-and-terrorism/general/docs/report_on_the_implementation_of_cfd_2008-919-jha_and_cfd_2002-475-jha_on_combating-terrorism_en.pdf [Accessed 4 June 2020].
55 Rec. 10 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. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].
56 Op. cit., Rec. 10 and 40.
Interestingly, the wording of the proposal of online terrorist content regulation is not so strict, stipulating:

“the expression of radical, polemic or controversial views in the public debate on sensitive political questions should not be considered terrorist content.”

The scope of freedom of speech, when it comes to terrorist propaganda, remains blurred due to many indefinite legal terms used, which might be problematic regarding principles of foreseeability and unambiguity of criminal law. These principles are meant to secure that a person has to know whether she would commit a crime by particular act.

3.2. COUNTER-TERRORISM DIRECTIVE AND HOSTING SERVICE PROVIDERS’ OBLIGATIONS

Legal persons may be held criminally liable for public provocation to commit a terrorist offence under the conditions of Art. 17 (1) (2) of the Counter-Terrorism directive. The provision is particularly important to hosting service providers (hereinafter as “HSP”) as they enable uploading third party content. It is strictly stipulated that a legal person may be held liable in the situation where the lack of supervision or control by a person in the particular leading position has made possible the commission of public provocation to commit a terrorist offence, for the benefit of the legal person by a person under its authority.

The obligation to remove or to block online terrorist content is imposed as a preventive measure and is presumed to be adopted promptly.

---

57 Rec. 9 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

58 For the complexities of the right to the free speech on the internet in different jurisdictions, see Lessig, L. and Resnick, P. (1999) Zoning Speech on the Internet: A Legal and Technical Model. *Michigan Law Review*, p. 395–396. Available from: https://cyber.harvard.edu/wg_home/uploads/200/1999-06.pdf [Accessed 16 May 2020]; Barnhizer for example describes the U.S. approach to the limitations on free speech with the phrase “sticks and stones can break the bones but words can never hurt”, in comparison to the European world in which “the beliefs of many ethnic and religious groups are closely related to pride, honor and shame.” Barnhizer, D. R. (2007) Reverse Colonization: Islam, Honor Cultures and the Confrontation between Divine and Quasi-Secular Natural Law. Cleveland-Marshall Legal Studies Paper No. 07-142, p. 5. Available from: https://ssrn.com/abstract=980687 [Accessed 16 May 2020].

59 Art. 21 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. *Official Journal of the European Union*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].
i.e. without any link to criminal or other proceedings. It is expressly stipulated that no general obligation to monitor transmitted or stored information nor to actively seek out the facts or circumstances indicating illegal activity should be imposed on service providers. The actual knowledge of illegal activity and awareness of the facts is still essential for their liability.\(^\text{60}\) Although no obligation regarding private monitoring is imposed, the endeavours are welcomed. The Counter-Terrorism directive presumes either public or judicial action, enhancing particularly voluntary action of the Internet industry,\(^\text{61}\) such as forming the Global Internet forum to Counter Terrorism by Facebook, Microsoft, Twitter and YouTube in July 2017\(^\text{62}\) or the cooperation of Facebook, Twitter, Google and Microsoft in using the software PhotoDNA to detect extremist online content, such as violent terrorist imagery or recruitment videos.\(^\text{63}\) The cooperation is based on sharing an industry database of “hashes”, i.e. unique digital fingerprints for violent terrorist imagery or videos that have been removed from their services. Only the most extreme content is shared in the database, the one most likely to violate all of the respective companies’ content policies.\(^\text{64}\)

Even though the number of HSP who have put in place measures dealing with terrorist content on their services rises, the Commission does not consider voluntary frameworks and partnerships sufficient enough, as not all affected HSP engaged in the voluntary cooperation.\(^\text{65}\) To speed up the procedures dealing with terrorist content on the services of information society service providers in the EU, a new regulation on preventing the dissemination of terrorist content online has been proposed.

---

\(^\text{60}\) Op. cit., Rec. 23.

\(^\text{61}\) Op. cit., Rec. 22.

\(^\text{62}\) GIFCT. Global Internet Forum to Counter Terrorism: Evolving an Institution. [online] Available from: https://gifct.org/about/ [Accessed 16 May 2020].

\(^\text{63}\) Facebook. (2016) Partnering to Help Curb Spread of Online Terrorist Content. [press release] 5 December. Available from: https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorism-content/ [Accessed 16 May 2020].

\(^\text{64}\) Ibid.

\(^\text{65}\) Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final), p. 1. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].
4. PROPOSAL FOR A NEW REGULATION ON PREVENTING THE DISSEMINATION OF TERRORIST CONTENT ONLINE

Legal basis for the new regulation should be Art. 114 of the Treaty on the functioning of the EU providing for the adoption of measures approximating the establishment and functioning of the internal market.66 Although the proposed provisions are primarily focused to tackle online terrorist propaganda, the Commission itself repeats the motive to intervene against the dissemination of terrorist content. Chosen legal basis and alleged obstacles for economic activity in the EU as the main goal of new regulation are rather questionable. The first paragraph of the explanatory memorandum itself refers to the terrorist attacks and the misuse of internet by terrorists aiming to glorify their atrocities.67 Nevertheless, a proclaimed goal of the legislation is:

“to guarantee the smooth functioning of the Digital Single Market, whilst ensuring trust and security.”68

By setting a minimum set of obligations for the HSP directing their services to the EU, the Commission believes in preventing the misuse of internet for terrorist purposes, improving accountability and transparency of HSP offering services in the EU, and clarifying their liability rules.69 New regulation should lead to detection and removal or blocking of online terrorist content by the HSP offering services in the EU irrespective of their place of main establishment.70 However, the scope of applicability is narrowed by a definition of “to offer services in the EU” and by demanding either an establishment in the EU, a significant number of users, or targeting the activities to at least one member state.71

Liability benefit in Art. 14 of the E-commerce directive72 stipulating specific conditions under which HSP are not liable for the stored

---

66 Op. cit., p. 4.
67 Op. cit., p. 1.
68 Op. cit., p. 3.
69 Op. cit., p. 2. See also Art. 1 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].
70 Art. 1 (2) Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].
71 Op. cit., Art. 2 (3).
information, should not be affected by any pro-active measures adopted on the basis of the regulation.\textsuperscript{73} However, Art. 15 (1) of the E-commerce directive expressly specifies that no general obligation to monitor the transmitted or stored information, nor to actively seek facts or circumstances indicating illegal activity shall be imposed on HSP. The prohibition of general monitoring in the E-commerce directive compared with the proactive monitoring for terrorist content online shows a clear change of perception on the necessary level of virtual freedom. Even though Rec. 19 of the Proposal proclaims that any proportionate and specific proactive measures should not present a general obligation to monitor,\textsuperscript{74} it is also mentioned that grave risks of terrorist content dissemination may justify a derogation from this principle under the EU framework and the HSP shall take proactive measures against the dissemination of terrorist content.\textsuperscript{75} The negotiating position of the Council of the EU adopted on 6 December 2018 which agreed on the proposed rules, is also signaling the shift in the attitude towards monitoring illegal and harmful online content.\textsuperscript{76}

On the other hand, the European Parliament (hereinafter as “EP”) in the legislative resolution of 17\textsuperscript{th} April 2019 on the Proposal, adopted many amendments aiming to emphasize the freedom to receive and impart information and ideas in an open and democratic society, the rule of law and the perception of terrorist content as a part of a broader problem of illegal content online, and the general obligation for HSP to monitor

\textsuperscript{72} Art. 14 of the 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. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549827901048&uri=CELEX:32000L0031 [Accessed 16 May 2020]. (hereinafter as “E-commerce directive”)

\textsuperscript{73} Rec. 5 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

\textsuperscript{74} Op. cit., Rec. 19.

\textsuperscript{75} Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final), pp. 3–5. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

\textsuperscript{76} Council of the EU. (2018) Terrorist Content Online: Council adopts negotiating position on new rules to prevent dissemination. [press release] 6 December. Available from: https://www.consilium.europa.eu/en/press/press-releases/2018/12/06/terrorist-content-online-council-adopts-negotiating-position-on-new-rules-to-prevent-dissemination/ [Accessed 16 May 2020].
stored information or to actively seek facts indicating illegal activity has been refused.\(^{77}\)

Although the Proposal introduces a completely new definition of terrorist content on the basis of the Counter-Terrorism directive, it does not have an impact on definitions of terrorist offences set in the Counter-Terrorism directive. Under Art. 2 (5) terrorist content should mean following information:

\(\begin{align*}
  & a) \text{ inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;} \\
  & b) \text{ encouraging the contribution to terrorist offences;} \\
  & c) \text{ promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Art. 2(3) of the directive on combating terrorism or} \\
  & d) \text{ instructing on methods or techniques for the purpose of committing terrorist offences.}^{78}\n\end{align*}\)

According to Art. 5 of the Counter-Terrorism directive the essence of public provocation to commit a terrorist offence is the message intending to incite commission of terrorist offence. The Proposal introduces a broader definition of terrorist content, which comprises inciting and advocating, but also promoting and instructing on the activities related to terrorist offences. Such definition enables to remove (or block access to) a wider set of online content particularly through the indefinite “activities” of a terrorist group. The EP’s amendments have narrowed the definition with the link to the terrorist offences in the Counter-Terrorism directive and the notion

---

\(^{77}\) Compare the Amendments 2–4, 6, 10, 12, 15, 21, 27, 43, 45, 46, 61, 62, 85, 86, 87, 88, 100, 103, 104, 106, 107, 110, 147 adopted by the EP. European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018) 0640 – C8-0405/2018 – 2018/0331(COD)). Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=EP:P8_TA(2019)0421 [Accessed 16 May 2020].

\(^{78}\) Art. 2(5) Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].
of intent, but did not clarify the activities of a terrorist group under Art. 2(5) c) of the Proposal.

Assessment of whether an information is or is not a terrorist content shall be done both by public authorities and HSP. Some rules are offered, but the guidance is only general. Overbroad definitions are criticised as the text introduces risks of arbitrariness in the removal of online content. Even though the Proposal enhances adoption of proactive measures regarding the monitoring of online content by HSP to prevent dissemination of terrorist content, the distinction of free speech and illegal terrorist content is not improved, while fundamental conditions could have been stipulated in terms and conditions of each HSP. The EP has deleted the latter provision that could be perceived as a step towards fragmentation of the freedom to receive and share information online.

HSP should apply measures to prevent dissemination of terrorist content and to determine what appropriate, proportionate and effective proactive measure should be put in place, while in the same time they are not encouraged to perform general monitoring. Empowering other bodies than judicial to decide on the implemented measures has been criticised by the Committee on Internal Market and Consumer Protection of the European Commission.

---

79 Amendment 53, 54. European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD)). Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=EP:P8_TA(2019)0421 [Accessed 16 May 2020].

80 Op. cit., Amendment 55.

81 Rec. 9 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

82 EDRI. (2018) The EU Council’s general approach on Terrorist Content Online proposal: A step towards pre-emptive censorship. [press release] 11 December. Available from: https://edri.org/the-eu-councils-general-approach-on-terrorist-content-online-proposal-a-step-towards-pre-emptive-censorship/ [Accessed 16 May 2020].

83 See Art. 3 (2) Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

84 Amendment 63 European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD)). Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=EP:P8_TA(2019)0421 [Accessed 16 May 2020].

85 Rec. 16 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].
Parliament (hereinafter as “IMCO”). The IMCO has made amendments to Rec. 37 of the Proposal so that administrative authorities may only issue removal orders on the basis of a court decision, but may not impose penalties. A provision regarding a “competent authority” which shall mean only “a designated national judicial authority in the Member State”, has been added. The changes signalised distrust in the arrangement where non-judicial (public or private) authorities would gain broad powers in the online content supervision system. Consequently, the EP has amended Rec. 37 and proposed, that the competent authority shall be:

“a single designated judicial authority or functionally independent administrative authority in the Member State.”

Another obligation of HSP is to comply with legal order requesting to remove or to disable access to terrorist content within one hour from receiving the order from competent authority. Considerable financial penalties for the HSP who would fail to do so are suggested. The one-hour limit for the removal was regarded as too short and unrealistic. Therefore, the EP has obliged the HSP to remove terrorist content or disable access to it “as soon as possible”, but as the rule “within one hour from receipt of the removal order” has stayed, the obligation is even stricter. Choice of competent authority with the power to issue a removal order is on the member states;

86 Draft Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (2018/0331 (COD)). Available from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-632.028+01+DOC+PDF+V0//EN&language=EN [Accessed 16 May 2020].
87 Op. cit., Amendment 30.
88 Op. cit., Amendments 48, 88.
89 Amendment 60 European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – CS-0405/2018 – 2018/0331 (COD)). Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=EP:P8_TA (2019)0421 [Accessed 16 May 2020].
90 Art. 4 (2) Proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].
91 Op. cit., Art. 18 (4).
92 Draft Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (2018/0331 (COD)). Available from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-632.028+01+DOC+PDF+V0//EN&language=EN [Accessed 16 May 2020].
it could be single designated judicial authority or functionally independent administrative authority. Possibility to have removal orders issued from other than judicial authorities might be problematic as the removal orders can intervene with the right to share and receive information. Possible variant would be to have the public authority issue a removal order in preliminary proceedings. Interim and precautionary measures are typical in civil and criminal court proceedings throughout the EU and may be imposed on a defendant or an accused person by a court before the final judgement on the merits is rendered. As the removal orders according to Art. 4 (2) of the Proposal will definitely interfere with the right to the free speech and freedom to share and receive information, the competent authority with the power to issue them should be the court. On the other hand, courts are not specialised in particular agenda as the administrative bodies are, and court proceedings may be lengthier. A fast reaction needed to block or remove online terrorist content effectively could be jeopardized.

5. CONCLUSION
Manifestations of terrorists’ beliefs and activities are visible online as terrorists use online social media platforms to magnify impact of their acts or to promote their crimes publicly. Even though social contact is deemed more important for individual radicalisation, online terrorist propaganda plays a particular role. The HSP offering their services in the EU are encouraged to identify terrorist online content and to remove it immediately from all their respective services and platforms. Many HSP started to participate in voluntary frameworks and partnerships to share information and cooperate.

While the Counter-Terrorism directive focuses on harmonisation of terrorist offences’ definitions and obliges the EU member states to ensure prompt removal of such online terrorist content, the proposal of online terrorist content regulation clearly imposes the obligations to prevent dissemination of terrorist content online, including the choice of proactive

---

94 Op. cit., Amendment 60.
95 European Union. (2019) Interim and precautionary measures. European e-justice. [online] Available from: https://e-justice.europa.eu/content_interim_and_precautionary_measures-78-en.do?init=true [Accessed 16 May 2020].
measures, on HSP. Risks that the measures might unlawfully restrict the right to information have been described. The demands to define the limits between public provocation to commit a terrorist offence and the freedom of speech persist. The burden of assessment whether online information does or does not constitute a terrorist content will be shifted more on HSP who will become the actual jurors of legality. Even though this approach is understandable due to the immense amount of online information and the abuse of social platforms for terrorist propaganda and recruitment, risks for freedom to receive and impart information is apparent. There is a clear change of perception on the necessary level of online control and monitoring in the EU.

The approach of prioritizing security before liberties of digital society has led the Commission to present the proposal of online terrorist content regulation. Generally approving attitude of the Council on preventive regulation of the internet regarding online terrorist content and the changes in secondary legislation reflect considerable shift in the perception of individuals’ freedoms in online environment. The EP’s amendments, on the other hand, emphasized the liberties of online environment. Remedies ensuring due review of removal and blocking of alleged illegal online content must be secured. HSP should be encouraged to remove terrorist content online and to cooperate with member states’ law enforcement agencies and Europol. Nevertheless, implemented measures should be decided by the public authorities in the proceedings with a possibility of judicial review.

Balancing between liberty and security is persistent in the political environment since the terrorist attacks of 11 September 2001. In adopting specific counter-measures against the risk of terrorism, the analysis performed by decision makers is likely to be tilted towards the interest on security than the one on liberty. The terrorist attacks experienced during recent years have accelerated and influenced the legislative process in the EU significantly and might be leading to undervaluation of liberty, particularly the right to receive and impart information as a basic principle of information society.

96 Waldron, J. (2011) Safety and Security. *Nebraska Law Review*, 85. Available from: http://digitalcommons.unl.edu/nlr/vol85/iss2/5/ [Accessed 16 May 2020].

97 Gross, O. (2018) *Security vs. Liberty: An Imbalanced Balancing*. Minnesota Legal Studies Research Paper No. 09-42, pp. 2-3. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471634 [Accessed 16 May 2020].
LIST OF REFERENCES

[1] Arab Convention for the Suppression of Terrorism. Adopted by the Council of Arab Ministers of the Interior and the Council of Arab Ministers of Justice, 22 April 1998. Available from: http://www.unodc.org/images/tldb-f/conv_arab_terrorism.en.pdf [Accessed 16 May 2020].

[2] Barlow, J. P. (1990) Crime and Puzzlement: in advance of the law on the electronic frontier. Whole Earth Review.

[3] Barnhizer, D. R. (2007) Reverse Colonization: Islam, Honor Cultures and the Confrontation between Divine and Quasi-Secular Natural Law. Cleveland-Marshall Legal Studies Paper No. 07-142. Available from: https://ssrn.com/abstract=980687 [Accessed 16 May 2020].

[4] Broadhurst, R. et al. (2017) Cyber terrorism: research report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology. Available from: https://ssrn.com/abstract=2984101 or http://dx.doi.org/10.2139/ssrn.2984101 [Accessed 16 May 2020].

[5] Council Framework Decision of 13 June 2002 on combating terrorism and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. Official Journal of the European Union. Consolidated version available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002F0475-20081209 [Accessed 16 May 2020].

[6] Council of Europe Convention on the Prevention of Terrorism, 16 May 2005. Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808c3f55 [Accessed 16 May 2020].

[7] Council of the EU. (2018) Terrorist Content Online: Council adopts negotiating position on new rules to prevent dissemination. [press release] 6 December. Available from: https://www.consilium.europa.eu/en/press/press-releases/2018/12/06/terrorist-content-online-council-adopts-negotiating-position-on-new-rules-to-prevent-dissemination/ [Accessed 16 May 2020].

[8] 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. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549827901048&uri=CELEX:32000L0031 [Accessed 16 May 2020].

[9] 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. Official Journal of the European Union.
Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

[10] Draft Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (2018/0331 (COD)). Available from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-632.028+01+DOC+PDF+V0//EN&language=EN [Accessed 16 May 2020].

[11] EDRI. (2018) The EU Council’s general approach on Terrorist Content Online proposal: A step towards pre-emptive censorship. [press release] 11 December. Available from: https://edri.org/the-eu-councils-general-approach-on-terrorist-content-online-proposal-a-step-towards-pre-emptive-censorship/ [Accessed 16 May 2020].

[12] European Commission. (2008) The Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52014DC0554 [Accessed 16 May 2020].

[13] European Council. (2018) EU Counter-Terrorism Strategy. Available from: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/eu-strategy/ [Accessed 16 May 2020].

[14] European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 –2018/0331 (COD)). Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=EP:P8_TA (2019)0421 [Accessed 16 May 2020].

[15] European Union. (2019) Interim and precautionary measures. European e-justice. [online] Available from: https://e-justice.europa.eu/content_interim_and_precautionary_measures-78-en.do?init=true [Accessed 16 May 2020].

[16] EUROPOL. (2016) Changes in Modus Operandi of Islamic State (IS) Revisited. Available from: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited [Accessed 16 May 2019].

[17] EUROPOL. (2019) Internet Organised Crime Threat Assessment (IOCTA). Available from: https://www.europol.europa.eu/iocta-report [Accessed 16 May 2020].
[18] EUROPOL. (2019) The European Union Terrorism Situation and Trend Report 2019. Available from: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat [Accessed 16 May 2020].

[19] Facebook. (2016) Partnering to Help Curb Spread of Online Terrorist Content. [press release] 5 December. Available from: https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/ [Accessed 16 May 2020].

[20] Facebook. (2020) Facebook Q1 2020 Results. Investor Relations. [online] Available from: https://s21.q4cdn.com/399680738/files/doc_financials/2020/q1/Q1-2020-FB-Earnings-Presentation.pdf [Accessed 16 May 2020].

[21] GIFCT. Global Internet Forum to Counter Terrorism: Evolving an Institution. [online] Available from: https://gifct.org/about/ [Accessed 16 May 2020].

[22] Gross, O. (2018) Security vs. Liberty: An Imbalanced Balancing. Minnesota Legal Studies Research Paper No. 09-42. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471634 [Accessed 16 May 2020].

[23] Hilbert, M. and López, P. (2011) The World’s Technological Capacity to Store, Communicate, and Compute Information. Science, 332 (6025). Available from: http://science.sciencemag.org/content/332/6025/60 [Accessed 16 May 2020].

[24] Heinke, D. H. (2016) Countering Radicalisation and Recruitment of so-called Jihadists – Proscription of Radicalization Hubs. Defence Against Terrorism Revue, 8.

[25] Hunter, R. and Heinke, D. H. (2011) Radicalization of Islamist Terrorists in the Western World. FBI Law Enforcement Bulletin, 9 (80). Available from: https://leb.fbi.gov/articles/perspective/perspective-radicalization-of-islamist-terrorists-in-the-western-world [Accessed 16 May 2020].

[26] Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging. (2011) STL-11-01/1, Special Tribunal for Lebanon, 16 February 2011. Available from: https://www.refworld.org/cases,STL,4d6280162.html [Accessed 16 May 2020].

[27] Judgement of 31 January 2017, Lounani, C-573/14, ECLI:EU:C:2017:71.

[28] Lessig, L. and Resnick, P. (1999) Zoning Speech on the Internet: A Legal and Technical Model. Michigan Law Review. Available from: https://cyber.harvard.edu/wg_home/uploads/200/1999-06.pdf [Accessed 16 May 2020].

[29] National transposition measures communicated by the Member States concerning: 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. Available from: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32017L0541 [Accessed 16 May 2020].

[30] Plous, S. (1993) The Psychology of Judgement and Decision Making. New York: McGraw-Hill.

[31] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[32] Rediker, E. (2015) The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union. Michigan Journal of International Law, 36 (2). Available from: https://repository.law.umich.edu/mjil/vol36/iss2/3/ [Accessed 16 May 2020].

[33] Sanyal, S. (2015) International Laws to Control Terrorism: A Comparative Study. AAKROSH Asian Journal on Terrorism and Internal Conflicts. Available from: http://dx.doi.org/10.2139/ssrn.3232739 [Accessed 16 May 2020].

[34] Shamieh, L. and Szenes, Z. (2015) The Propaganda of ISIS/DAESH through the Virtual Space. Defence Against Terrorism Revue, 7 (1). Available from: http://www.coedat.nato.int/publication/datr/volumes/datr10.pdf [Accessed 16 May 2020].

[35] The Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (COM/2014/554 final). Available from: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/crisis-and-terrorism/general/docs/report_on_the_implementation_of_cfd_2008-919-jha_and_cfd_2002-475-jha_on_combating_terrorism_en.pdf [Accessed 4 June 2020].

[36] United Nations. (2019) New technologies, artificial intelligence aid fight against global terrorism. [press release] September 4. Available from: https://news.un.org/en/story/2019/09/1045562 [Accessed 16 May 2020].

[37] Waldron, J. (2011) Safety and Security. Nebraska Law Review, 85. Available from: http://digitalcommons.unl.edu/nlr/vol85/iss2/5/ [Accessed 16 May 2020].