BRIEFING

EU Legislation in Progress

European Parliament

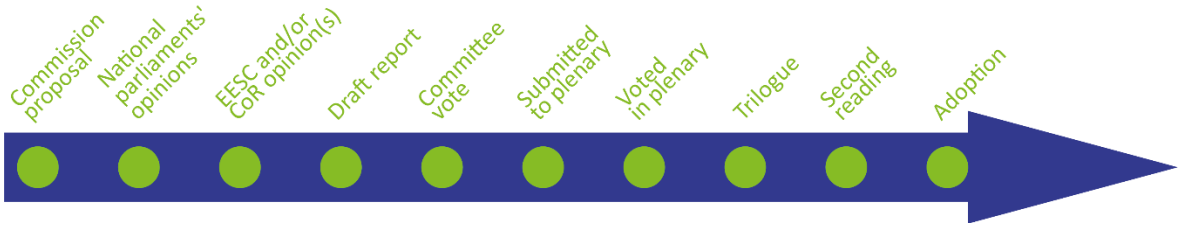
Addressing the dissemination of terrorist content online

OVERVIEW

Dissemination of terrorist content is one of the most widespread and most dangerous forms of misuse of online services in the field of internal security. In line with the 2015 European agenda on security, and taking into account the impact of this propaganda on the radicalisation, recruitment and training of terrorists, the European Commission launched a voluntary system for tackling terrorism online, based on guidelines and recommendations. However, given the limitations of self-regulation, in September 2018 the Commission proposed a regulation on preventing the dissemination of terrorist content online through the removal of such content within one hour of being posted.

While the Council rapidly reached a position on the proposal, the European Parliament adopted its first-reading position in April 2019. Following the European elections, and the appointment of a new rapporteur, interinstitutional trilogue negotiations on the proposal began in autumn 2019. The trilogue meetings were delayed several times, because of the coronavirus pandemic among other reasons. After a new series of terrorist attacks hit Europe in autumn 2020, Parliament and Council reached political agreement on 10 December 2020. The most contentious issues related to the cross-border effect of withdrawal orders and to the use of automated filters to detect terrorist content online. After the Council adopted the text on 16 March 2021, Parliament adopted it in plenary on 28 April. The Regulation entered into force on 6 June and will apply as of 7 June 2022.

Proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online		
Committee responsible:	Civil Liberties, Justice and Home Affairs (LIBE)	COM(2018) 640 12.9.2018
Rapporteur:	Patryk Jaki (ECR, Poland)	2018/0331(COD)
Shadow rapporteurs:	Javier Zarzalejos (EPP, Spain) Marina Kaljurand (S&D, Estonia) Maite Pagazaurtundúa (Renew, Spain) Jean-Paul Garraud (ID, France) Patrick Breyer (Greens/EFA, Germany) Cornelia Ernst (The Left, Germany)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Procedure completed.	Regulation (EU) 2021/784 OJ L 172, 17.5.2021, pp. 79-109	



EPRS | European Parliamentary Research Service

Author: Katrien Luyten
Members' Research Service

PE 649.326 – July 2021

EN

Introduction

The internet is a powerful communication tool that is also widely used to spread hatred, violence and terrorist propaganda. The influence of illegal content is so great that it has a key impact on the security of the Union, through terrorist threats and attacks. The digital environment offers easy ways to radicalise. Radicalisation processes are based on the same e-communication methods as any commercial brand: terrorist organisations and ideologies use marketing tools to spread their ideas more effectively. Recruitment propaganda, training materials, information and even live executions are disseminated online, often on a global basis and generally taking advantage of easy and quick access to this type of media. The internet is a remarkable networking tool, allowing the dissemination of any type of data, information or propaganda, simply through a hosting service provider (HSP).

Terrorism and radicalisation have been on the rise in the EU, in particular since the 2015 and 2016 terrorist attacks in Paris and Brussels. There has been a slight decline in the number of terrorist attacks since 2017, but the threat remains high and is becoming increasingly complex, as its nature evolves over time and poses multiple challenges to the EU and its Member States. Despite the defeat of ISIL/Da'esh on the ground, the online presence of Jihadi organisations, through their various magazines[1] and on social networks, remains high. Even though most fatalities in the EU and in the world are caused by jihadist terrorism, right-wing violent extremism is increasingly becoming a challenge. These groups also use internet tools to spread propaganda or to promote radicalisation and violent and terrorist action. The need for the authorities to do more to tackle the online propaganda coming from terrorist organisations or radicalised individuals more thoroughly and consistently and to improve the way such activities are monitored and addressed is therefore increasingly pressing.

Existing situation

Terrorism, along with organised crime and cybercrime, was made a priority in the 2015 European agenda on security. In December 2015, in line with a commitment made in the agenda on security, the Commission launched the EU Internet Forum, gathering Member States, Europol and internet industry representatives. It has since been completed by the Civil Society Empowerment Programme (CSEP), a network coordinated by the Radicalisation Awareness Network Centre of Excellence (RAN CoE) that partners civil society organisations with internet and social media companies with a view to fighting terrorist propaganda online and protecting vulnerable targets.

According to the European Commission,[2] Europol made over 50 000 decisions on referrals to service providers about terrorist content on their platforms between July 2015 and 2018. To mention just one example, the UK's Internet Referral Unit (CTIRU) alone identified 300 000 pieces of terrorist content between 2010 and 2018. However, some companies are taking proactive measures to identify terrorist content by themselves, referrals only account for a small proportion of the total content removed. For instance, the Commission noted in its impact assessment that Twitter suspended over 1.2 million accounts for violations of their terms of service in relation to the promotion of terrorism between August 2015 and December 2017 and Facebook took action on 1.9 million pieces of ISIL/Da'esh and al-Qaeda content in the first quarter of 2018.

International organisations, governments and private companies are also active in the field. For instance, in 2001 the Council of Europe (CoE) adopted the Convention on cybercrime and in 2005 the Convention on the prevention of terrorism. Given the threat resulting from the use of online tools for terrorist purposes, the CoE committee of experts on terrorism (CODEXTER), in cooperation with the Max Planck Institute, evaluated the situation in CoE member states with a view to providing recommendations on the problems created by a cyberterrorist context.

In 2017, the United Nations Security Council (UNSC), in its Resolution 2354 (S/RES/2354(2017)), validated the 28 April 2017 comprehensive international framework to counter terrorist narratives

(S/2017/375), which, in particular, quotes as examples the action of the EU Internet Forum and of the Civil Society Empowerment Programme. The framework also takes into account the UNSC resolutions imposing law enforcement obligations on UN countries 'that are relevant to countering terrorist narratives'.

In 2019, following the internet impact of the Christchurch attacks, heads of state or government and internet industry representatives met in Paris and adopted the Christchurch Call launched by French President Emmanuel Macron and New Zealand Prime Minister Jacinda Ardern. In 2017, Facebook, Microsoft, Twitter and YouTube created the Global Internet Forum to Counter Terrorism, and were joined in 2019 by Dropbox, Amazon and WhatsApp. The forum builds on the EU Internet Forum and is inspired by the Christchurch Call.

European Council and Council starting position

The European Council, in its June 2017 conclusions, considered that the online industry also needed to take responsibility. The Heads of State or Government expected industry to develop a forum based on the model of the EU Internet Forum, in order to develop new tools and improve automatic detection and removal of content inciting terrorist acts. The European Council also called for the adoption of relevant legislative measures at EU level. In its 28 June 2018 conclusions, the European Council welcomed 'the intention of the Commission to present a legislative proposal to improve the detection and removal of content that incites hatred and to commit terrorist acts'.

In June 2014, the Council revised the 2008 EU strategy for combating terrorism, taking into account in particular the use of social media by terrorists and it adopted related guidelines in December 2014. The following year, the Justice and Home Affairs Council mandated Europol to build a unit dedicated to reducing the level and impact of terrorist and violent extremism propaganda online: the European Union Internet Referral Unit (EU IRU) was established in July 2015. The EU Counter-Terrorism Coordinator, Gilles de Kerchove, is active in the field too, being involved in the EU Internet Forum and the Global Internet Forum to Counter Terrorism.

Parliament's starting position

On 15 June 2017, the European Parliament adopted a resolution on online platforms and the digital single market (2016/2276(INI)), insisting on the need to clarify the liability of intermediaries on online platforms, calling in particular on online platforms to take measures against illegal content online and welcoming the intention of the Commission to propose measures against such material in the then-ongoing work on the Audiovisual Media Services (AVMS) Directive (2018/1808). The European Parliament introduced amendments to the proposal for an AVMS Directive, adding references to content relating to incitement to terrorism, in accordance with the Article 5^3 of Directive (EU) 2017/541 on combating terrorism.

Preparation of the proposal

In September 2017, the European Commission adopted a communication setting out guidelines and principles on the prevention, detection and removal of illegal content online, including hatred, violence and terrorist propaganda. In March 2018, it adopted a recommendation, including a set of non-binding operational measures to be taken by online providers and Member States to tackle illegal content online. Based on the principle that 'what is illegal offline is illegal online', it defined illegal content as any information that is not compliant with EU or Member State law. The recommendation also indicated how to flag and process illegal content and listed a set of measures aimed at reducing the spread of online terrorist propaganda. It sought notably to forbid the hosting of terrorist propaganda and to create the obligation to remove it within an hour of being flagged by law enforcement authorities or Europol.

Following this recommendation in 2018, the Commission conducted an open public consultation. Its results confirmed that most respondents considered the internet to be safe and were keen to

protect online freedom of speech. Hosting service providers were open to cooperation with law enforcement authorities and preferred voluntary measures to regulatory interventions. Associations insisted on the need for targeted measures and civil-rights-oriented organisations expressed concerns. Intellectual property rights owners supported greater responsibility for HSPs and academics emphasised the wide range of illegal content online.

This consultation was accompanied in 2018 by a Flash Eurobarometer on illegal content online that touched upon hate speech, child sexual abuse material, incitement to terrorism, consumer scams and content infringing intellectual property rights.

The European Commission went a step further with the 2018 State of the European Union (SOTEU) address, which announced a proposal for a regulation aimed at getting terrorist content offline within an hour. The Commission President at the time, Jean-Claude Juncker, considered this proposal to be a priority[4] in his 2018 letter of intent to the European Parliament President, Antonio Tajani, and to Chancellor Sebastian Kurz, representing the Austrian Presidency of the Council. The proposal was issued on 12 September 2018 (COM(2018) 640), on the same day as the SOTEU address.

Legal framework

The proposal is based on Article 114 TFEU on the establishment and functioning of the internal market and not on the provisions defined in Title V of the Treaty, relating to the area of freedom, security and justice, and in particular in Article 83(1). According to the proposal, Article 114 is appropriate as the proposal is designed to harmonise the conditions for HSPs to provide cross-border services in a way that will address the differences between Member States without impacting on the functioning of the internal market. Under Article 114 it would also be possible to impose obligations on HSPs established outside the EU, in cases where their activities affect the internal market. The Commission chose to propose a regulation as this will avoid divergent transposition and provide for uniform application across the Union.

The proposal has taken into account the principles set by the digital single market strategy and refers to the e-Commerce Directive (2000/31/EC), as it does not result in HSPs losing the liability exemption provided for under Article 14[5] of the above-mentioned directive. A decision to impose proportionate and specific measures should not – in principle – lead to the imposition of a general obligation to monitor as defined by Article 15(1)[6] of the e-Commerce Directive. The proposal has been prepared in accordance with the definition of terrorist offences mentioned in Article 3(1) of the 15 March 2017 Directive on Combating Terrorism (2017/541). Illegal terrorist content is therefore defined as information that is used to incite and glorify the committing of terrorist offences, encourage the contribution to and provide instructions for committing terrorist offences, or promote participation in terrorist groups.

Among the principles that guided the preparation of the proposal, the Commission refers to the above-mentioned 2017 and 2018 European Council conclusions and to the 2017 Parliament resolution on online platforms and the digital single market. The proposal also refers to respect for fundamental rights, in particular the freedom of expression and information, and the right to effective judicial compensation.

Impact assessment

According to the impact assessment accompanying the proposal, terrorist content online is a multifaceted security challenge, as HSPs have to face a complex legal framework at Member State level. This situation is complicated by the fact that in its Article 3 the e-Commerce Directive establishes the principle of the country of origin, according to which HSPs have to comply with the law of the State in which they are established. This principle derives from the digital single market strategy, under which EU Member States are not allowed to restrict digital services from another Member State, unless it is necessary and proportionate to protect objectives of public policy, public security, public health or protection of consumers. Member States have underlined the dispersal of

terrorist content across a greater number of smaller service providers as an emerging trend posing a persistent security challenge.

The Commission insists on the urgency of the regulation, as voluntary actions against terrorist content online have proven insufficient. It also takes into account the social and economic impact of the proposal on HSPs, in particular SMEs, aiming to avoid measures that would limit their competitiveness or confront them with new forms of red tape. When it comes to fundamental rights, the impact assessment notes that the proposal could have both positive and negative impacts: negative in terms of freedom to do business, of expression and information, the right to data protection and respect for private life; positive, however, on the right to life as a result of increased security. It also examines coherence with the e-Commerce Directive and the Directive on Combating Terrorism. The proposal targets HSPs established in the EU as well as outside it, if they propose services in the EU. The initial appraisal of the Commission impact assessment produced by EPRS, considers that the impact assessment clearly identifies the main problems together with their drivers and consequences. It finds the analysis of impacts to be somewhat limited, however, due to a lack of available data.

The changes the proposal would bring

- The proposal is aimed at countering the security threat represented by the continuous flow of terrorist content online, through all categories of platform. The voluntary measures adopted by HSPs were considered not sufficient and therefore the Commission proposes to enhance the action against terrorist content online by means of a mandatory legal framework applicable to all industry players. The proposal focuses on HSPs offering their services in the European Union, 'regardless of their place of establishment or their size'. It seeks to ensure that when terrorist content is identified, it is taken down as early and as quickly as possible, that online platforms take measures against the misuse of their services, and that removed content is not re-uploaded elsewhere. The one-hour rule: the Commission is proposing a legally binding one-hour deadline for content to be removed following a removal order from national competent authorities.
- Terrorist content is defined as material that incites or advocates the committing of terrorist offences, promotes the activities of a terrorist group or provides instructions and techniques for committing terrorist offences.
- A duty of care obligation is imposed on all platforms to ensure that they are not misused for the dissemination of terrorist content. Given a possible risk of dissemination via their platforms, HSPs might also be required to take proactive measures to protect their platforms and their users from terrorist abuse.
- A framework for strengthened cooperation between hosting service providers, Member States and Europol is to involve HSPs and Member States designating points of contact reachable at all times to facilitate follow-up to removal orders and referrals.
- HSPs will be able to rely on effective complaint mechanisms that all service providers will have to put in place. Where content has been removed unjustifiably, the service provider will be required to reinstate it as soon as possible. Effective judicial remedies will also be provided by national authorities, and platforms and content providers will have the right to challenge a removal order. For platforms making use of automated detection tools, human oversight and verification should be in place to prevent erroneous removals.
- Transparency and accountability will be supported by annual reports, and Member States will have to put in place financial penalties for non-compliance with removal orders, possibly amounting to as much as 4 % of the provider's global turnover of the previous business year.

One of the difficulties of such a regulation is that its provisions are always close to the limit when it comes to fundamental rights – in particular, the rights to freedom of expression and information. In addition, there are technical issues and questions of compliance with other legislation. The proposal refers to the 15 June 2017 Parliament resolution on online platforms and the digital single market. It does not mention the AVMS Directive however.

Advisory committees

The European Economic and Social Committee (EESC) opinion (SOC/609-EESC-2018) welcomes the initiative on preventing terrorist content online and highlights the need to combat the dissemination of terrorist information and digital recruitment on social networks. The EESC however highlights the need to guarantee the effective right to information and freedom of expression on the internet in the EU. Fighting radicals online will boost trust in the internet and this should improve the development of the sector. However, the Committee points to the need to assess the possible impact of the proposal on small and medium-sized companies, in particular to avoid distorting competition with bigger players. Direct action by civil society organisations and citizens is necessary and should involve developing counter-narratives, and helping social media to take proactive measures to promote reporting, in order to have a preventive effect.

National parliaments

As of 31 January 2020, six national parliaments had provided contributions to the debate:

- the Romanian Chamber of Deputies, welcomes the procedure as described in the proposal, notably supporting the safeguard measures on fundamental rights; it recommends Member States share best practices to avoid radicalisation; it underlines, however, the possible damage to freedom of expression and opinion that could result from the proposal and the possible impact the proposal could have on business. In particular, Member States should not check for personal data that they should not retain, and sanctions should be applied by Member States in a unified manner.
- The German Bundesrat shares the apprehension of the European Commission on the dissemination of terrorist content online and welcomes the principle of such a proposal. However it casts doubt on the legal basis of the proposal, given that, in its opinion, Article 114 TFEU relates to the internal market and does not cover the security issues covered by the proposal; it also criticises the fact that there is a risk that the future regulation could only apply to the most important players in the sector, and suggests that derogations to the one-hour rule should apply to SMEs. The Bundesrat also has doubts as to the compliance of the proposal with the e-Commerce Directive.
- The Spanish Congress of Deputies considers that HSPs willing to offer their services on EU territory must comply with clear rules to avoid their services being misused for the purpose of distributing terrorist content online. It considers that the proposal will help to ensure the swift removal of terrorist content online and is fundamental in ensuring the security of European citizens. The scale and effect of the intended action mean that its objectives could not be reached by the Member States at central, regional or local level and for that reason the proposal upholds the subsidiarity principle.
- The Portuguese Parliament[7] considers that the proposal complies with the principles of subsidiarity and proportionality and deems it important to follow up on further legislative and political developments regarding the issue, in particular through exchanges of information between the national and EU institution levels.
- The Romanian Senate (EN/RO) considers that the proposal does not comply with the principle of proportionality, as the Directive on Combating Terrorism (541/2017) has not yet been transposed in all Member States, it is not possible to base the proposal on a unified definition of terrorist offences and thus develop related sanctions. It also considers that the proposal may create a restriction to the freedom of expression; the

Senate does not agree with the possible effect of the proposal, given that the forbidden content might be posted again, generating repeated costs and effort for national authorities.

- The Czech Senate (EN/CZ) supports the idea of preventing terrorist content online; however it underlines uncertainties with regard to the link between the proposal and the e-Commerce Directive.

Stakeholder views

Before launching the proposal, several consultations carried out by the European Commission garnered views and comments on the issue. HSPs, while acknowledging the negative impact of terrorist content on their services, put the focus on the considerable volume of illegal content online and the difficulty combating it. The recent decrease in the volume of terrorist content online is both attributed to ISIL/Da'esh's difficulties and to efforts undertaken by Member States and EU internet referral units, as well as those made by the HSPs on a voluntary basis.

Stakeholder organisations representing business, human rights organisations, and EU-based and non-EU-based organisations had the opportunity to express their views at the beginning of the legislative procedure.

- Online businesses and industry representatives belonging to the DigitalEurope trade association supported the principle of fighting terrorist content online and welcomed the possible impact of the proposal on the dissemination of such content. They considered that cloud infrastructure providers should not be included in the scope of the future regulation. They called for a more flexible deadline for removing content. For DigitalEurope, the future regulation should not prescribe mandatory measures but facilitate better cooperation between service providers and law enforcement authorities. The Cloud Infrastructure Service Providers (CISPE), meanwhile, considered that cloud infrastructure should not be targeted by the proposal, which was not, according to this organisation, adapted to their industry.
- EDRi (European Digital Rights), which represents human rights organisations in the digital domain, saw the proposal as 'election-motivated policy-making'. One of EDRi's concerns related to 'the extension of the upload filter regime the EU is currently about to introduce for copyright to terrorist content'. It stated that 'requiring internet companies to monitor everything we say on the web does not only have grave implications for the freedom of speech, but it also follows a dangerous path of outsourcing and privatising law enforcement'. EDRi proposed a number of amendments to the proposal in line with their principles.
- APC (the Association for Progressive Communications) issued an open letter in January 2019 to the members of the LIBE committee asking them to oppose the proposal. It raised concerns about the protection of human rights based on the 2018 document from the UN Special Rapporteurs on Human Rights. APC noted that in 2017 the International Criminal Court issued an arrest warrant on a case based on videos found on the internet.
- CDT (the Centre for Democracy and Technology) considered that the text adopted by the plenary improved the initial proposal 'significantly'.
- AmCham EU, the American Chamber of Commerce in the EU, made several comments regarding the definition of terrorist content. It requested flexibility on the one-hour rule and considered that there was a need for 'legal certainty around what the proactive measures should entail'. For AmCham EU, proactive measures were only necessary for HSPs that had been exposed to terrorist content. The scale of financial sanctions could lead to restrictions of freedom of speech due to over-zealous HSPs.

Expert views

Experts and academics also had the opportunity to express their views on the proposal.

- In December 2018, three Special Rapporteurs,[8] independent experts of the United Nations Human Rights Council (UNHRC), expressed concerns about the proposal even though they recognised the need for action to prevent the dissemination of terrorist content online. The definition of content was too broad in their opinion. For them, the best way to prevent internet platforms from being used for terrorist purposes would be for the public authorities and HSPs to work together, using international human rights law and the UN Guiding Principles on Business and Human Rights.
- In February 2019, the EU Fundamental Rights Agency (FRA) released an opinion, as requested by the LIBE committee, on the fundamental rights implications of the proposal. FRA considered that the definition of terrorist content needed to be modified, as it broadened the terms of the Directive on Combating Terrorism (2017/541); the definition of terrorist content was considered too wide and would interfere with the freedom of expression and information; the proposal did not guarantee any type of involvement by the judiciary. Moreover, FRA considered that the Member States' obligation to protect fundamental rights online had to be strengthened, as well as the principle of due diligence.
- In February 2019, the European Data Protection Supervisor (EDPS) sent 'formal comments' on the draft regulation to the Parliament, the Council and the Commission proposing 'possible improvements, in order to significantly reduce any possible conflict with the fundamental rights to privacy and to the protection of personal data'.
- Professor Jan Bernd Nordemann, a German copyright law specialist, questioned whether the preventive duties of HSPs were in line with EU law. The European Commission released a study on hosting intermediary services and illegal content online, on the scope of Article 14 of the e-Commerce Directive, which applies to many more services than in 2000. The study gives an interpretation of the duty of care, notably by trying to clarify the intention of the lawmakers. Dr Gavin Robinson also commented on the proposal, as did Jordy Krasenberg, an RAN CoE expert, who underlined the fact that terrorist content online requires – in the eyes of the EU – a combination of legislative, non-legislative, and voluntary measures based on collaboration between authorities and HSPs with respect for fundamental rights.

Legislative process

Before the 2019 European elections

Council

In December 2018, the Justice and Home Affairs Council agreed on a general approach on the proposal, thus adopting its negotiating position. Several provisions were added or modified by the Member States. For instance, in terms of duties of care, the Council added in Article 3(2) that HSPs must include in their terms and conditions that they will not store terrorist content. A new article, 4(a), was added on the consultation procedure for removal orders. In the recitals, the Council pointed out that the regulation should not apply to activities relating to national security as this remained the sole responsibility of each Member State. The possibility for HSPs to contest a decision imposing proactive measures or penalties before a court of the Member State in which they were established or had legal representation was added to the right to an effective remedy.

European Parliament

The proposal was assigned to the Committee on Civil Liberties, Justice and Home Affairs (LIBE), with the Committee on Culture and Education (CULT) as associated committee and with the Committee

on Internal Market and Consumer Protection (IMCO) also giving an opinion. The Committee on Industry, Research and Energy (ITRE) decided not to give an opinion. LIBE first appointed Helga Stevens (ECR, Belgium) as rapporteur, replaced in December 2018 by Daniel Dalton (ECR, UK). CULT appointed Julie Ward (S&D, UK) as rapporteur for opinion. IMCO appointed Julia Reda (Greens/EFA, Germany) as rapporteur for opinion.

After receiving the amendments from the various committees, the debate and vote on the draft report took place in LIBE on 8 April 2019. One of the issues raised was compliance of the proposal with the e-Commerce Directive and the AVMS Directive. The plenary adopted amendments to the proposal at first reading on 17 April 2019. As proposed, HSPs could face sanctions of up to 4 % of their global turnover if they systematically and persistently fail to abide by the legislation on terrorist content. The text includes no obligation to monitor or filter content, even though service providers would be obliged to withdraw illegal content within an hour. The text adopted targets material that encourages the committing – or contributes to the committing – of terrorist offences, for instance by providing instructions or guides on how to produce and use explosives, firearms and other weapons for terrorist purposes. Furthermore, amendments clarify the definition of 'terrorist content' and provide exceptions for smaller platforms.

Since the 2019 elections

The file was included on the list of unfinished business to be carried over to the European Parliament's ninth term (2019-2024). The trilogue negotiations with the Council and the Commission therefore became the responsibility of the European Parliament elected in May 2019. A new rapporteur, Patryk Jaki (ECR, Poland) was appointed on 4 September 2019 by the LIBE committee. Julie Ward (S&D, UK) was appointed as rapporteur by CULT as associated committee and was then replaced by Petra Kammerevert (S&D, Germany) following the UK's withdrawal from the EU on 31 January 2020. The IMCO committee appointed Marcel Kolaja (Greens/EFA, Czechia) as rapporteur for opinion. The LIBE committee decision of 24 September 2019 to enter into interinstitutional negotiations was announced in the plenary, on 9 October 2019.

Interinstitutional negotiations

The first trilogue meeting was held on 17 October. In its 20th progress report towards achieving a Security Union, the Commission - on 30 October - called on the co-legislators to reach agreement on the proposal by the end of 2019. Further trilogue meetings were held on 20 November and 12 December, as well as several technical meetings, but they could not solve the differences of opinion between the Council and the Parliament negotiators. The most controversial issues included:

- the one-hour rule, with the Council insisting on the need to react quickly for the rule to be effective;
- the use of proactive measures and tools such as algorithms and other content filters by HSPs, with Parliament being against such mandatory generalised surveillance;
- the cross-border scope of the removal order, with the Council insisting on retaining direct jurisdiction of a national authority over a platform based in another Member State;
- the nature of the authority issuing the removal order, which Parliament insisted had to be a competent judicial or independent authority;
- the definition of the scope of 'terrorist content', with Parliament insisting on exceptions for educational and journalistic content;
- accommodations for small businesses, where Parliament feared the regulation would be difficult to implement by medium-sized platforms and SMEs;
- penalties, in particular those that affect the target company's turnover.

The trilogue meeting scheduled for 18 March 2020 had to be cancelled because of the coronavirus pandemic. Doubts about secure videoconferencing solutions – as an alternative to physical

meetings – and the summer recess led to the postponement of further trilogue meetings until 24 September. Despite the long interval between trilogue meetings, according to a state-of-play report from the Council of 3 July, work continued in technical trilogues and during Justice and Home Affairs Counsellors meetings. The Commission had submitted compromise proposals with regard to the most contentious issues on 6 March. Provisional agreement was reached on several issues during the technical meetings but could only be confirmed at a full trilogue meeting. Upon Parliament's request, the Council accepted that the title of the regulation be changed to 'Regulation on addressing the dissemination of terrorist content online' as opposed to 'preventing'. Common ground still needed to be found on the definition of terrorist content, the articles concerning HSPs' duties of care and proactive measures, the scope of cross-border removal orders and the designation of competent authorities, as well as on the penalties.

The next trilogue meeting took place on 29 October but in spite of being close to an agreement, the negotiators could not finalise the text. A new series of terrorist attacks in Europe that autumn, increased the urgency to wrap up. Reacting to the recent events and commemorating the fifth anniversary of the terrorist attacks in Paris, on 13 November, EU home affairs ministers reiterated their commitment to completing the negotiations on the proposal by the end of 2020. During a sixth trilogue meeting, on 10 December, the co-legislators then agreed on the outstanding issues and reached political agreement on the proposal.

The agreement

In the agreed final text, the definition of terrorist content is fully aligned with that of the Directive on combating terrorism. It concerns materials such as texts, images, sound recordings or videos, including live transmissions, that incite, solicit or contribute to terrorist offences, provide instructions for such offences or solicit people to participate in a terrorist group. The regulation also aims to combat content that provides guidance on how to make and use explosives, firearms and other weapons for terrorist purposes.

The agreement upholds the one-hour rule. Voluntary cooperation with HSPs will continue, but, as was requested by Parliament, the competent authorities in the Member State in which the HSP has its main establishment have the right to scrutinise the removal order and to block its execution if they consider it violates fundamental rights. In practice, this means that the terrorist content identified in the removal order has to be removed or access to it has to be disabled in all Member States within one hour of receipt of the injunction, but the authority of the Member State in which the HSP is located has 72 hours to analyse and possibly challenge the withdrawal order. Depending on the decision taken after the challenge, the content either becomes available again or is permanently deleted. HSPs and content providers will have 48 hours to contest the removal order from the country of origin.

The agreement also includes exceptions when material is disseminated for educational, journalistic, artistic or research purposes, or to prevent or counter terrorism. This also includes content expressing critical or controversial views in a public debate. Furthermore, there will be no general obligation for internet platforms to monitor or filter content, except when they are exposed to terrorist content. In that case the HSP decides on the measures to take but there will be no obligation to use automated tools. Those HSPs that have taken action against the dissemination of terrorist content in a given year will have to publish transparency reports on the action taken. The Member States themselves will lay down the rules on penalties in case of non-compliance with the legislation, taking into account the nature, gravity and duration of the infringement, as well as whether the infringement was intentional or negligent.

On 11 January 2021, the LIBE committee approved the agreed text. The Council subsequently adopted the text at first reading on 16 March. Parliament then adopted the text at second reading - without a vote, as no amendments to the text were put forward - during its April plenary session. The rapporteur qualified the regulation during the final debate as 'a good outcome that balances security and the freedom of speech and expression on the internet, protects legal content and

access to information for every citizen in the EU, while fighting terrorism through cooperation and trust between states'. European Commissioner Ylva Johansson added: 'Without online manuals to tell you how, it's harder to make bombs. Without flashy propaganda videos, it's harder to poison the minds of young people. Without streaming attacks online, it's harder to inspire copycat attacks. It's difficult to measure: people are not radicalised, bombs not made, attacks not carried out. We may never be able to count how many, but this regulation will save lives'. The new regulation entered into force on 6 June 2021 and will apply as of 7 June 2022.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS

Boucher P. et al., Polarisation and the use of technology in political campaigns and communication, STOA, EPRS, European Parliament, March 2019.

Dalli H., Preventing the dissemination of terrorist content online, initial appraisal of a European Commission impact assessment, EPRS, European Parliament, January 2019.

Eriksson E. et al., Radicalisation and violent extremism – focus on women: How women become radicalised, and how to empower them to prevent radicalisation, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, December 2017.

Milt K. et al., Countering terrorist narratives, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, November 2017.

Quaglio G. et al., Harmful Internet use - Part II: Impact on culture and society, STOA, EPRS, European Parliament, January 2019.

Van Ballegooij W. and Bąkowski P., The fight against terrorism - Cost of non-Europe report, EPRS, European Parliament, May 2018.

Voronova S., Understanding EU counter-terrorism policy, EPRS, European Parliament, January 2021.

OTHER SOURCES

Preventing the dissemination of terrorist content online, European Parliament, Legislative Observatory (OEIL).

ENDNOTES

[1] Bunker R. and Ligouri Bunker P., Radical Islamist English-language online magazines, August 2018.

[2] European Commission, Impact assessment accompanying the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, SWD(2018) 408, 12 September 2018.

[3] This article provides that 'Member States shall take the necessary measures to ensure that 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 causing a danger that one or more such offences may be committed, is punishable as a criminal offence when committed intentionally'.

[4] Priority 7.

[5] Article 14.

'1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.'

[6] Article 15(1): Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

[7] Please save the linked document and open it with Acrobat Reader.

[8] Special Rapporteurs: Prof. David Kaye on the promotion and protection of the right to freedom of opinion and expression, Prof. Joseph Cannataci on the right to privacy and Prof. Fionnuala Ní Aoláin on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Third edition of a briefing originally drafted by François Théron. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.