



Council of the
European Union

Brussels, 3 March 2021
(OR. en)

Interinstitutional File:
2018/0331(COD)

14308/20
ADD 1

CT 122
ENFOPOL 355
COTER 121
JAI 1135
CYBER 285
TELECOM 281
FREMP 149
AUDIO 70
DROIPEN 127
CODEC 1412

DRAFT STATEMENT OF THE COUNCIL'S REASONS

Subject: Position of the Council at first reading with a view of the adoption of a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE
COUNCIL on addressing the dissemination of terrorist content online
– Draft Statement of the Council's reasons

I. INTRODUCTION

1. On 12 September 2018, the Commission submitted the abovementioned proposal¹ for a Regulation on preventing the dissemination of terrorist content online to the Council and the European Parliament. The legal basis is Article 114 [Approximation of laws] of the Treaty on the Functioning of the European Union, and the proposal is subject to the ordinary legislative procedure.
2. The European Economic and Social Committee (EESC) was consulted by the Council by letter of 24 October 2018 and delivered its opinion on the proposal on 12 December 2018² during its December plenary session.
3. On 6 December 2018, the Council agreed on a general approach³ on the TCO which constituted the mandate for the negotiations with the European Parliament in the context of the ordinary legislative procedure.
4. On 12 February 2019, the European Data Protection Supervisor sent ‘formal comments’ on the draft Regulation to the European Parliament, the Commission and the Council⁴. On the same day, the European Union Agency for Fundamental Rights, following a request from the European Parliament of 6 February 2019, issued an opinion on the proposal⁵.
5. On 17 April 2019, the European Parliament adopted a first-reading position⁶ on the Commission proposal, with 155 amendments to the Commission's proposal, and with 308 votes in favour to 204 against, with 70 abstentions.

¹ 12129/18 + ADD 1-3.

² OJ C 110, 22.3.2019, p. 67 (15729/19).

³ 15336/18.

⁴ Ref. 2018-0822 D2545 (WK 9232/2019).

⁵ FRA opinion - 2/2019 (WK 9235/2019).

⁶ See 8663/19 (Information note from GIP2 (Inter-institutional Relations) to COREPER presenting the outcome of the European Parliament's first reading); the Parliament's mandate was confirmed by the plenary on 10-11 October 2019.

6. The Council and the European Parliament entered into negotiations in October 2019 with a view to reaching an early second reading agreement. The negotiations were successfully concluded on 10 December 2020 with the European Parliament and Council reaching a provisional agreement on a compromise text.
7. On 16 December 2020, COREPER II analysed and provisionally confirmed the final compromise text in view of the agreement reached with the European Parliament⁷.
8. On 11 January 2021, the compromise was endorsed by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE). On 13 January, the Chair of the LIBE Committee addressed a letter to the Chair of COREPER II to inform him that, should the Council transmit formally to the European Parliament its position in the form presented in the Annex to that letter, he would recommend to the Plenary that the Council's position be accepted without amendment, subject to legal-linguistic verification, at the European Parliament's second reading⁸.

⁷ 12906/20.

⁸ 5634/21.

II. OBJECTIVE

9. The Regulation provides a clear legal framework that sets out the responsibilities of Member States and hosting service providers with a view to addressing the misuse of hosting services for the dissemination of terrorist content online, guaranteeing the smooth functioning of the Digital Single market, whilst ensuring trust and security in the online environment. In particular, it seeks to provide clarity as to the responsibility of hosting service providers for ensuring the safety of their services and for swiftly and effectively addressing, identifying and removing or disabling access to terrorist content online. It creates a new and effective operational instrument for the elimination of terrorist content by enabling the issuing of removal orders, that have cross-border effect. In addition the aim is to maintain safeguards to ensure the protection of fundamental rights, including the freedom of expression and information in an open and democratic society and the freedom to conduct a business. The Regulation provides that terrorist content be removed within a maximum of one hour from the receipt of the removal order, and sets out online platforms' responsibilities in ensuring the removal of such content. In addition to judicial redress possibilities guaranteed by the right to an effective remedy, the Regulation introduces a number of safeguards and complaint mechanisms.
10. The competent authority/ies of each Member State can issue a removal order to any hosting service provider offering services within the EU. The competent authority/ies in the Member State where the service provider has its main establishment will have the right - and upon the reasoned request by hosting service providers or content providers the obligation - to scrutinise the removal order if the removal order is deemed to seriously or manifestly violate the Regulation itself or infringe upon fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union. Member States should adopt the rules on penalties for infringements of the obligations, taking into account, amongst other things, the nature thereof and the size of company in question.

III. ANALYSIS OF THE COUNCIL'S POSITION AT FIRST READING

GENERAL

11. The European Parliament and the Council conducted negotiations with the aim of concluding a second-reading agreement on the basis of a Council first-reading position that the Parliament could approve as such. The text of the Council Position at first reading on the Regulation on preventing the dissemination of terrorist content online fully reflects the compromise reached between the two co-legislators, assisted by the European Commission.

SUMMARY OF THE MAIN ISSUES

12. Following a request from the European Parliament, the title of the Regulation was changed to "Regulation on addressing ~~preventing~~ the dissemination of terrorist content online".
13. The definition of "terrorist content" is consistent with the definitions of the relevant offences under the Directive on combating terrorism⁹. Concerning the scope, the Council's first-reading position covers materiel disseminated to the public, *i.e.* to a potentially unlimited number of persons. Materiel disseminated for educational, journalistic, artistic or research purposes or for awareness-raising purposes to prevent or counter terrorism should not be considered terrorist content. This also includes content expressing polemic or controversial views in a public debate on sensitive political questions. An assessment shall determine the true purpose of the dissemination. It has also been specified that the Regulation shall not have the effect of modifying the obligation to respect the rights, freedoms and principles referred to in Article 6 TEU and shall apply without prejudice to fundamental principles relating to freedom of expression and information, including freedom and pluralism of the media.

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 (OJ L 88, 31.3.2017, p. 6).

14. Hosting service providers shall take appropriate, reasonable and proportionate measures to effectively address the misuse of their service for the dissemination of terrorist content online. If hosting service providers are exposed to terrorist content, they will have to take specific measures to protect their services against its dissemination. The text agreed merges three Articles - Article 3 (Duties of care), Article 6 (Proactive measures) and Article 9 (Safeguards in relation to proactive measures) - into one on "Specific measures". The choice of those measures is a matter for the individual hosting service provider. The Council first-reading position makes it clear that the hosting service provider can use different measures to address the dissemination of terrorist content, including automated measures, which can be adapted to the abilities of the hosting service provider and the nature of services offered. Where the competent authority considers that the specific measures put in place are insufficient to address the risks, it will be able to require the adoption of additional appropriate, effective and proportionate specific measures. However, the requirement to implement such additional specific measures should not lead to a general obligation to monitor or to engage in active fact-finding within the meaning of Article 15(1) of Directive 2000/31/EC¹⁰ or to an obligation to use automated tools. In order to secure transparency, hosting service providers will have to publish annual transparency reports on action taken against the dissemination of terrorist content.
15. The role of the host Member State in relation to removal orders with cross-border effects has been strengthened, by introducing a scrutiny procedure: the competent authority of the Member State where the hosting service provider has its main establishment or legal representative may, on its own initiative, scrutinise the removal order issued by competent authorities from another Member State in order to determine whether or not it seriously or manifestly infringes the Regulation or the fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union. At the reasoned request of a hosting service provider or a content provider, the host Member State is obliged to scrutinise if there is such an infringement.

¹⁰ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

16. Except in duly justified emergency cases, a 12-hour advance notification including information on the applicable procedures and deadlines, should be given to those hosting service providers that have not previously received a removal order from that authority, in particular with a view to alleviating the burden on small and medium-sized enterprises (SMEs).
17. The Article on referrals - a mechanism for alerting hosting service providers of terrorist content for the providers' voluntary consideration against its own terms and conditions - is deleted, but a recital clarifies that referrals remain at the disposal of Member States and Europol.
18. Terrorist content which has been removed or access to which has been disabled as a result of removal orders or of specific measures must be preserved for six months from the removal or disabling, a period which can be prolonged if and for as long as necessary in relation to a review.
19. Member States shall lay down rules on penalties applicable to infringements by the hosting service providers of the Regulation. Penalties could take different forms, including formal warnings in the case of minor infringements or financial penalties in relation to more severe infringements. The Council first-reading position sets out which infringements are subject to penalties and which circumstances are relevant for assessing the type and level of such penalties. Hosting service providers could face sanctions of up to 4% of their global turnover if they systematically or persistently fail to abide by the one-hour rule to remove or disable access to terrorist content.

IV. CONCLUSION

20. The Council's position fully reflects the compromise reached in the negotiations between the European Parliament and the Council, and facilitated by the Commission. This compromise is confirmed by the letter from the Chair of the European Parliament's LIBE Committee Affairs addressed to the Chair of COREPER II, dated 13 January 2021.