

Brussels, 26 November 2020 (OR. en)

12959/20

LIMITE

JAI 973 CATS 86 COSI 205 COPEN 322 FREMP 118 EUROJUST 143 EJN 96

NOTE

From:	Presidency
To:	Delegations
Subject:	Presidency discussion paper on aspects of terrorism

Delegations will find attached a discussion paper by the Presidency on five aspects relating to terrorism:

- 1. Council conclusions on the European arrest warrant
- 2. Victims of terrorism
- 3. Cumulative prosecution of foreign terrorist fighters for core international crimes and terrorism-related offences
- 4. Digitalisation
- 5. Hate speech online

This version of the paper takes account of suggestions presented at Coreper on 25 November 2020.

12959/20 SC/sl 1
JAI.2 **LIMITE EN**

PRESIDENCY DISCUSSION PAPER ON ASPECTS OF TERRORISM

The recent attacks in France and Austria have demonstrated that terrorism remains a serious threat in the EU. A wide range of measures have already been taken in the field of justice to improve the EU's capacity to fight terrorism. While some of the instruments adopted focus on terrorism, many of our most successful tools have a wider scope. The current efforts belong in both categories and include (1) the constant improvement of the functioning of the European arrest warrant, (2) efforts to better support victims of terrorism, (3) analysis of the grounds to successfully prosecute foreign terrorist fighters, (4) digitalisation (using digital tools to cooperate more efficiently and accessing electronic evidence) and (5) the fight against hate speech online which feeds extremism, radicalisation and terrorism.

The objective of this document is to present a state of play on these issues and invite Ministers to discuss these efforts, with a greater focus on the issue of hate speech online.

1. Conclusions 'The European arrest warrant and extradition procedures - current challenges and the way forward'

The European arrest warrant (EAW) is a key instrument in the fight against terrorism. The functioning of the EAW is overall satisfactory and particularly efficient in criminal procedures related to terrorist offences. However, its operation can still be improved, taking into account the case-law of the CJEU.

Informal agreement was reached on working level on Council conclusions on the European arrest warrant and extradition procedures. Areas for improvement include:

^{13214/20.}

- a) The national transposition and practical application of the EAW Framework Decision. Under this point, the conclusions among other things call on the Member States to remedy shortcomings in their national legislation that hamper the effectiveness of the Framework Decision and invite them to lay down non-binding guidelines for its application. It is underlined that the Commission has started infringement procedures and, where necessary, will continue initiating such proceedings in the near future. Further, the conclusions highlight the need to support and increase continuous training for practitioners and invite the Commission to update the EAW Handbook in the near future.
- b) More support should be given to executing authorities in dealing with fundamental rights evaluations. Under this point, the conclusions note that the case-law of the CJEU has given practitioners the challenging task of resolving the tension between mutual recognition and the protection of fundamental rights on a case-by-case basis. Among other things, the conclusions invite the Commission to provide more attention in the EAW Handbook to the issue of fundamental rights, and invite the FRA to regularly update its criminal detention database.
- c) Certain aspects of the procedure in the issuing and executing Member State. Under this point, the conclusions among other things invite the Member States to consider whether they could make greater use of the possibility to accept translations in one or more other official languages of the European Union than they do at present. Further, the Commission is invited to adopt a three-step approach when considering the need and advisability of presenting a legislative proposal on the transfer of proceedings in criminal matters.
- d) Finally, on strengthening EAW surrender procedures in times of crisis, the conclusions underline among other things that the COVID-19 pandemic has clearly illustrated the need for the prompt and comprehensive digitalisation of cross-border judicial cooperation.

2. <u>Victims of terrorism</u>

Supporting victims of terrorism and strengthening their rights are a fundamental part of our European values and must be an integral part of European counter-terrorism policy. Against this background, the Presidency has placed particular emphasis on the issue of support for victims of terrorism, especially in cross-border situations, and has - as a result of its work - issued a Presidency report on the issue². The topic has been discussed with Member States and experts in the field at a high-level conference on victims' rights, as well as at five meetings of the COPEN Working Party.

On the basis of existing Union law on the rights of victims³ and the recently adopted EU Strategy on victims' rights (2020-2025)⁴, best practices and challenges in supporting victims of terrorism have been identified. Referring back to the Council Conclusions on victims of terrorism⁵, the Presidency further elaborated on the definition of national contact points for victims of terrorism, which Member States were called upon to nominate. National or "single" contact points for victims of terrorism are central structures in Member States that should guide victims after a terrorist attack, particularly in situations with a cross-border context. A number of Member States have already set up such contact points, several others are planning to do so soon.

The discussions in the Council regarding the structure, role and tasks of such national contact points have led the Presidency to make a number of recommendations on these aspects. Furthermore, the Presidency recommends that a network of single contact points for victims of terrorism could be organised at European level, for example through integration of such a network in the European Network on Victims' Rights (ENVR).

² 13175/20 (to be issued).

See in particular Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA; Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims and 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.

⁴ EU Strategy on victims' rights (2020-2025), COM (2020) 258, 24 June 2020 (9178/20).

⁵ Council conclusions on victims of terrorism, 4 June 2018 (9719/18).

The list of contact details of the single contact points for victims of terrorism that has been drawn up by the Presidency can serve as a basis for a future network of single contact points for victims of terrorism. As further steps, close cooperation with existing structures such as the European Commission Coordinator for victims' rights, Victims' Rights Platform and the European Centre of Expertise for victims of terrorism need to be ensured to avoid duplication. All these recommendations aim to facilitate the support for victims of terrorism across Europe.

3. <u>Cumulative prosecution of foreign terrorist fighters for core international crimes and terrorism-related offences</u>

ISIS, which has been classified as a terrorist organisation, has perpetrated horrific acts of violence in armed conflicts in Northern Iraq and Syria. The issue of investigating and prosecuting its members and foreign terrorist fighters returning to their countries of origin has led most EU Member States to focus on preventing and punishing terrorism-related offences. However, ISIS should not only be considered as a terrorist organisation. Under international humanitarian law, ISIS could also be treated as a party to a non-international armed conflict, acting as an organised non-state armed group.

Therefore, its members could be responsible for committing war crimes and other core international crimes and be the subject of **cumulative prosecutions**. The same applies to other terrorist organisations.

The subject of cumulative prosecutions was extensively discussed by practitioners with expertise in core international crime as well as in counter-terrorism on 6-7 November 2019 at the 27th meeting of the European network of contact points in respect of persons responsible for genocide, crimes against humanity and war crimes (the Genocide Network), and these discussions continued at the 5th EU Day Against Impunity for genocide, crimes against humanity and war crimes on 23 May 2020.

Subsequently, the secretariat of the Genocide Network prepared an expert report entitled 'Cumulative prosecution of foreign terrorist fighters for core international crimes and terrorism-related offences'. The report focusses on foreign terrorist fighters (FTFs), although the assessments regarding in particular the possibilities for cumulative prosecution are relevant to any member of these terrorist organisations, irrespective of his or her nationality.

The report demonstrates that existing national jurisprudence of Member States makes it possible to cumulatively prosecute and hold FTFs accountable for war crimes, crimes against humanity and the crime of genocide, in addition to terrorism-related offences. In some Member States, cumulative prosecution (terrorism and war crimes) could take place for the same facts. In others, cumulative prosecution could concern the same person, but for different facts.

The report concludes that prosecuting terrorism offences combined with acts of core international crimes ensures the full criminal responsibility of perpetrators, results in higher sentences and delivers more justice for victims.

4. <u>Digitalisation</u>

Digitalisation has an impact on criminal procedures related to terrorist offences, both regarding the access to electronic evidence and regarding the use of digital tools to improve and speed up judicial cooperation.

Cross-border access to e-evidence:

Efforts are ongoing to ensure a more efficient mechanism for cross-border access to e-evidence - this is crucial for a large part of today's criminal investigations, including cases of terrorism, given the current state of digitalisation. These efforts aim to supplement the internal EU rules with an instrument allowing MS competent authorities to request e-evidence <u>directly</u> from service providers active within the EU irrespective of their place of establishment and data location.

⁶ ST 12237/20, which has been presented to the members of CATS.

The instrument will remedy some of the challenges of existing channels of cooperation, e.g. the sometimes long response time in mutual legal assistance requests and possible inadmissibility of data obtained in voluntary cooperation. The Council adopted its position in December 2018 (draft Regulation) and in March 2019 (draft Directive) and is awaiting the adoption of the EP's final position. It is essential to begin the inter-institutional negotiations on this internal package and ensure that practitioners obtain an efficient tool as judicial and law enforcement authorities are confronted on a daily basis with difficulties in accessing electronic evidence.

Further, the EU is engaged in two sets of international negotiations pursuing similar objectives, for which the Commission was given the negotiating mandate in June 2019. The first is the ongoing negotiation on a second additional protocol to the Budapest Convention, whereas the second negotiation is with the US, due to the dominant position of US-based service providers and the need to settle conflicts of law. Progress on the latter is dependent on progress on the internal EU rules to ensure that norms and standards of protection are aligned.

The four negotiating rounds held so far have focussed on issues such as the parties' general objectives and positions, the scope of application of the agreement and safeguards. A date for a next round has not been set yet. Regarding the negotiations on the second additional protocol in the Council of Europe, despite steady progress on a number of protocol provisions (expedited disclosure of stored computer data in an emergency, access to the WHOIS data, etc.), some difficulties have arisen concerning the data protection safeguards and with regard to special regulations for federal states. The Council of Europe Secretariat proposed a renewed extension of the mandate until May 2021, as despite intensive negotiations, a conclusion is no longer expected by the end of the year. The Commission is actively working in both the protocol drafting group/plenary and the sub-groups on the protocol structure and data protection. The urgency of concluding the negotiations on the protocol stems not only from the need to provide practitioners with an instrument which is better adapted to the digital era, but also in view of the recently started preparations at the UN for a new international treaty on cybercrime.

Digitalisation of judicial cooperation in criminal justice:

It is of utmost importance that judicial cooperation in criminal matters is efficient if terrorism is to be addressed effectively. Efficiency in this area can be increased through further digitalisation of cross-border judicial cooperation. The COVID-19 pandemic has underlined that there is an urgent need for the prompt and comprehensive digitalisation of cross-border judicial cooperation.

A lot of work has already been done by the Commission and the Member States to set up the e-Evidence Digital Exchange System (e-EDES). This tool provides for secure, swift and efficient cross-border exchange of European Investigation Orders, mutual assistance requests and evidence in digital format. It is, therefore, important that all Member States establish a connection to the System without undue delay. eEDES should be gradually enriched and extended to other judicial cooperation instruments in criminal matters.

In December 2018, Eurojust presented a note to the Council outlining the need for a standardised set of digital tools to support efficient interaction and judicial cooperation within the European Union. Subsequently, in July 2019, the Commission initiated a study on digital criminal justice. The aim of the study was to better understand the business needs of the judicial community working on cross-border criminal cases, and to assess how these needs could be met by technological solutions.

The study 'Cross-border Digital Criminal Justice', which was presented in September 2020 and welcomed by all Member States, identifies seven broad categories of business needs:

- 1) stakeholders participating in judicial criminal cross-border cooperation need to securely communicate and exchange information via digital means;
- 2) interoperability across different systems needs to be ensured;
- 3) stakeholders need to easily manage the data and ensure its quality;
- 4) stakeholders investigating a given case should be able to identify links between cross-border cases;

- 5) data protection principles need to be respected for all systems;
- 6) create an online collaborative platform to support the setting up and operation of JITs;
- 7) access to the necessary digital tools should be ensured.

The study presents seven solutions to address these business needs and to implement the digital criminal justice concept: a secure communication channel, a communication tool, a redesigned Eurojust case management system, a JIT collaboration platform, the exchange of data between the JHA agencies and EU bodies, a cross-check of judicial cases, and a solution for large files.

While the first three solutions can be developed on the basis of existing technological solutions, the last four solutions will need a new technological solution (or a new task force).

The Commission is now working on these solutions and intends to present proposals in the final quarter of 2021, which will include a revision of the current Union legal framework on the exchange of information on counter-terrorism matters with Eurojust and the creation of a digital collaboration tool for Joint Investigation Teams (JITs).

5. Hate speech online

Introduction

The recent terrorist attacks in Europe have also illustrated - once again - the extent to which illegal hate speech poses a threat to the security of our citizens: incitement to violence and hatred and the dissemination of propaganda through social media platforms increasingly play a harmful role in the run up to and aftermath of such attacks. While the Union recognises and promotes freedom of expression, it is important to note that the Internet cannot be a safe haven for illegal hate speech. Law enforcement and judicial authorities rely on cooperation with online service providers to effectively investigate and prosecute criminal offences.

Current EU framework to tackle illegal hate speech online

The Framework Decision on Racism and Xenophobia (2008/913/JHA)⁷ defines a common criminal law approach to racist and xenophobic hate speech and hate crimes. In its EU anti-racism action plan for 2020-2025⁸, the Commission announced that it would make a comprehensive effort to ensure the correct transposition and implementation of the Framework Decision, particularly where the definition of hate speech or the criminalisation of hate crime have not been correctly transposed into national law.

On 31 May 2016, the Commission presented together with Facebook, Microsoft, Google (YouTube) and Twitter a 'Code of conduct on countering illegal hate speech online' whereby IT companies committed to review valid removal notifications of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary.

There have been five monitoring rounds on which the Commission has reported to the Council. The last one⁹, whose results were published in June 2020, showed that on average 90 % of the notifications are reviewed within 24 hours and 71 % of the content is removed.

On 1 March 2018, the Commission adopted a Recommendation on measures to effectively tackle illegal content online¹⁰ which presents a set of operational measures to be taken by companies and Member States to tackle all forms of illegal content online.

Finally, a proposal for a Regulation on preventing the dissemination of terrorist content online (TCO) was submitted by the Commission in September 2018. The proposal is still under discussion between the Council and the European Parliament. The German Presidency intends to conclude the trilogue negotiations in December 2020 in order to achieve a new system for cross-border instruments to ensure that illegal terrorist content is removed very rapidly while maintaining effectice safeguards for the protection of fundamental rights.

⁷ OJ L 328, 6.12.2008, p. 55–58.

⁸ 11522/20.

https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

^{10 6717/18.}

Possible next steps

Illegal hate speech on social media platforms poses a particular challenge to our societies. The recent terrorist attacks illustrate this, just as the COVID-19 pandemic has triggered new forms of hate speech that constitute criminal offences such as threats, incitement to violence or defamation.

The Union is committed to upholding freedom of expression, in line with the Charter of Fundamental Rights and the European Convention on Human Rights. Yet what is illegal offline should be illegal online. Internet companies hosting such content must take responsibility for illegal content or the misuse of their platforms. This responsibility entails an obligation to cooperate with law enforcement and judicial authorities.

As regards illegal content on social media platforms, the European Commission has now announced its intention to revise the existing legal framework for online service providers established by the e-Commerce Directive and to put forward a Digital Services Act that is expected to place greater responsibility on online service providers for illegal content posted by users. These issues give rise to complex legal questions as to the balance between the freedom of expression and the security of our citizens, but also as to how to effectively prosecute any criminal offences in that context.

As part of the upcoming debate on the responsibility of online platforms, a key element will be to define the obligations incumbent upon them with regard to law enforcement. This could imply an obligation to inform authorities of certain categories of criminal offences detected by the platforms in order to adequately ensure the security of our citizens and the prosecution of illegal hate speech. Any such obligations would have to be carefully framed in relation to possible impacts on fundamental rights of online service users, including freedom of expression, the right to private life and data protection. Access by law enforcement and judicial authorities to the digital evidence required for such prosecution also needs to be ensured. The e-evidence package will significantly contribute already to the first step: obtaining the data that is necessary for the identification of the author (including the IP address) of hate crimes committed on the platforms, but it needs to be ensured that the relevant content is not deleted after having been taken down.

A further issue to be considered concerns the understanding of illegal hate speech. The Framework Decision on Racism and Xenophobia provides for minimum rules on offences related to incitement to hatred or violence but they are not applicable to hatred or violence relating to gender, political affiliation or sexual orientation. Even where approximation exists, it seems that there are considerable differences between Member States regarding the legislation and the case law.

These differences could create specific challenges for the platforms themselves, for any authority that would need to decide whether the platforms are meeting their obligations and for law enforcement and judicial authorities when it comes to investigating and prosecuting hate speech and taking other action against offences perpetrated online. An intelligent mix of minimum harmonization and additional national legislation and enforcement with regard to the definition of illegal hate speech may be a way forward.

In the 2020 State of the Union and in its work programme for 2021, the Commission has announced a proposal to include hate crimes in the list of offences requiring approximation under Article 83(1) TFEU.

Questions:

In light of recent events and against this background, the German Presidency would like to put forward the following questions:

- 1. Do you have experience at national level regarding an obligation for the platforms to report criminal offences related to hate crime and hate speech to the competent authority if they become aware of such offences?
- 2. Would you consider it appropriate to provide for such an obligation or for other elements of a legal framework at EU level to fight illegal hatecrime and hate speech?
- 3. Do you see any other action which the EU should take to improve our fight against terrorism in the sectors mentioned above or in other sectors related to justice?