ARTICLES

SHAPING THE FUTURE OF EUROPE – SECOND PART
edited by Sandra Hummelbrunner, Lando Kirchmair, Benedikt Pirker, Anne-Carlijn Prickartz *and* Isabel Staudinger

THE EU RESPONSE TO TERRORIST CONTENT ONLINE: TOO LITTLE, (MAYBE NOT) TOO LATE?

VIVIANA SACHETTI*

ABSTRACT: The prevention and suppression of terrorist crimes within the European Union are subject of discussion at the European level, currently characterised by a heterogenous substantive framework that bears the risk of an insufficient response, particularly with regards to the massive spreading of terrorist content online. Indeed, while Directive 2017/541/EU provides a comprehensive discipline on the deterrence and repression of terrorist conducts, the EU is only just starting to address the specific problem of the illicit use of the internet by terrorists. Thus, the Commission's initiative to extend the competences of the European Public Prosecutor's Office (EPPO) to transnational terrorist crimes has timely recognised how the EU lacks a European level of prosecution and any compelling power towards domestic authorities. This creates gaps in investigations and proceedings in one Member State that may result in casualties or risks in the Union as a whole. This *Article* argues that the EPPO should consequently represent the central authority entrusted with the power to directly enforce instructions upon national prosecutors and to coordinate their joint actions in the field. This *Article* also suggests that Eurojust and Europol's capability as specialised agencies in this area should be enhanced on the basis of their well-established expertise on the subject.

KEYWORDS: Area of Freedom Security and Justice – Eurojust – European Public Prosecutor's Office – internet – judicial cooperation – terrorism.

* PhD Student in European Union Law, Università degli Studi Roma Tre, viviana.sachetti@uniroma3.it. This *Article* was originally presented at the 3rd Young European Law Scholars Conference, 'Shaping the Future of Europe' (Salzburg 27-28 February 2020).

www.europeanpapers.eu
ISSN 2499-8249
doi: 10.15166/2499-8249/509

I. Introduction

> "The quality of judicial cooperation in the fight against terrorism is a big challenge. We cannot work in silos in our countries anymore. We need an overall approach".[1]

This *Article* focuses on the current and foreseeable response to the challenges brought forward by the ever-growing terrorism threat within the EU legal order, particularly for what concerns its online dissemination.

Terrorist crimes perpetrated through or facilitated by the internet are current subject of discussion by EU Institutions and agencies, also in light of the increasing attention on tackling online disinformation.[2] Remarkably, public incitement to terrorism on the internet constitutes a crime under recent Directive 2017/541/EU,[3] which concerns the deterrence and suppression of terrorist conducts and requires Member States to adopt measures in order to ensure a swift removal of terrorist content online. Furthermore, this issue has been addressed both at the political level, during the 2018 European Council held in Salzburg, and at the legislative one, in the 2018 Commission's Proposal for a Regulation on preventing the spreading of such material.[4]

This creates a heterogenous substantive framework that bears the concrete risk of an insufficient response to the massive spreading of terrorist content online. Notably, the EU is considering the necessity of facing unitedly the grave threats posed by those crimes which can be perpetrated quite easily through the internet. Indeed, the Commission has already forwarded to the European institutions an initiative to extend the

[1] F Molins, former District Chief Prosecutor of Paris and leader of the investigation following the Paris terrorist events from 2015 onwards, at the 20 June 2018 Eurojust press conference on counterterrorism.

[2] While the Covid-19 pandemic will most likely contribute to an acceleration in the adoption of new means of protection against the threat of online disinformation, a number of instruments on the subject are already being considered. See, most recently, Communication COM(2020) 456 final of May 2020 from the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Europe's Moment: Repair and Prepare for the Next Generation; Communication COM(2020) 67 final of February 2020 from the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's Digital Future; Joint Communication JOIN(2020) 5 final of March 2020 from the European Parliament and the Council, EU Action Plan on Human Rights and Democracy 2020-2024.

[3] Directive 2017/541/EU 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. For a comprehensive overview on the developments adopted in the Directive compared to the previous Council Decision 2005/671, see J Maliszewska-Nienartowicz, 'A New Chapter in the EU Counterterrorism Policy? The Main Changes Introduced by the Directive 2017/541/EU on Combating Terrorism' (2017) PolishYIL 185 ff.

[4] Commission Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, COM(2018) 640 final. The Proposal was adopted by the European Parliament at its first reading of 17 April 2019 with a number of amendments which do not entail any major revisions of the original text.

competences of the European Public Prosecutor's Office (EPPO)[5] to cross-border terrorist crimes.[6] Several reasons stand in favour of this proposal, as further demonstrated; however, the classical approach to terrorism therein adopted shall be discarded, emphasising instead the internet's role both in the Commission and in the suppression of those criminal conducts, and further analysing its interplay with Eurojust and Europol.

This *Article* is divided in three main parts. First, it focuses on the results that the EU has already achieved on the substantive level in light the adoption of the abovementioned acts, also considering the subsequent legislation on the subject. Second, it addresses the opportunity of an implementation of the recent Communication by the Commission on the initiative to extend the competences of the EPPO to cross-border terrorist crimes. The third part discusses how the EU could further build upon the Commission's proposal, benefitting from the solid structure of Eurojust and Europol in order to increase the suppression of terrorist conducts, particularly within the internet, thus providing a high level of cybersecurity within its territory.

II. The fight against the dissemination of terrorist content online: a substantive framework

In the most recent years, the EU has offered both Member States and stakeholders – for instance, online hosting providers – a relevant framework on the prevention and suppression of terrorist conducts, through legislative measures (the already mentioned Directive 2017/541/EU and the Proposal for a Regulation on terrorist content online) and non-binding instruments (the Commission Recommendation (EU) 2018/334[7] and several voluntary agreements entered into by States or stakeholders[8]).

Directive 2017/541/EU[9] considers the appropriateness of harmonising national provisions on terrorism with the purpose of ensuring a high level of security within the EU

[5] Council Regulation (EU) 1939/2017 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ("the EPPO").

[6] Communication COM(2018) 641 final from the Commission to the European Parliament and the European Council of 12 September 2018, A Europe that protects: an initiative to extend the competences of the European Public Prosecutor's Office to cross-border terrorist crimes. A contribution from the European Commission to the Leader's meeting in Salzburg on 19-20 September 2018 (hereinafter 2018 Communication on the extension of the EPPO's competences).

[7] Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online of 1 March 2018.

[8] See for instance European Commission, *Fighting Terrorism Online: Internet Forum pushes for automatic detection of terrorist propaganda* (6 December 2017) ec.europa.eu; Europol, *Europol's EU Internet referral unit partners with Belgium, France and The Netherlands to tackle online terrorist content* (2 March 2018) www.europol.europa.eu.

[9] For a comment on Directive 2017/541/EU see A Garrido Muñoz, 'The Proposal for a New Directive on Countering Terrorism: Two Steps Forward, How Many Steps Back?' (2016) European Papers www.europeanpapers.eu 759.

territory, as well as better complying with the international obligations on the subject. Indeed, art. 3 of the Directive enlists several conducts that shall be deemed as terrorist to the extent that they are committed with the intention of *i)* intimidating a population, *ii)* compelling a government to perform a certain act, or *iii)* destabilising "the fundamental political, constitutional, economic or social structures of a country or an international organization".[10]

Public incitement to terrorism holds fundamental relevance in the Directive. Indeed, art. 5 requires Member States to "take the necessary measures to ensure that the distribution, or otherwise making available by any means, whether online or offline" of messages amounting to intentional provocation to commit terrorism related acts is considered as a punishable criminal offence by the national legislation.[11] Moreover, according to art. 21 of the Directive, the responsibility of ensuring the swift removal or blockage of "online content constituting a public provocation to commit a terrorist offence" lies with the States in the event that such content is hosted within their territory.

States should also strive to obtain the removal of this content when hosted on online platforms based in servers of other countries: however, it is not clear how national authorities may achieve this objective. The wording on the subject is indeed quite obscure and does not allow a univocal interpretation on whether this part of the provision refers to all States or to EU ones only.

Furthermore, as to Member States more specifically, this may imply an antinomy with art. 3 of the Directive 2000/31/EC ("eCommerce Directive"),[12] which provides a complex procedure regulating the interferences with another State's free movement of

[10] Pursuant to art. 3(1)(j), a mere threat to commit the acts therein listed is to be considered a terrorist conduct. This may concretely entail that conducts such as the threat of interfering illegally with an informatic system (art. 3(1)(i) reach the intensity of criminal contempt). Accordingly, such crime is punished with no less than a maximum penalty of eight years of imprisonment if the defendant directs a terrorist group, pursuant to art. 15(3) of the Directive.

[11] As provided by Recital 10 of the Directive 2017/541/EU cit.: "[s]uch conduct should be punishable when it causes a danger that terrorist acts may be committed. In each concrete case, when considering whether such a danger is caused, the specific circumstances of the case should be taken into account, such as the author and the addressee of the message, as well as the context in which the act is committed". See also S De Coensel, 'Incitement to Terrorism: The Nexus Between Causality and Intent and the Question of Legitimacy – A Case Study of the European Union, Belgium and the United Kingdom' in C Paulussen and M Scheinin (eds), *Human Dignity and Human Security in Times of Terrorism* (Springer 2020) 277 ff.; N Paunović, 'New EU Criminal Law Approach to Terrorist Offences' in D Duić and T Petrašević (eds), *EU and Comparative Law Issues and Challenges Series* (Faculty of Law, Josip Juraj Strossmayer University of Osijek 2018) 534-535.

[12] 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"). For a perspective on the need to amend this legislation in order to more adequately face the new technological challenges, see D Calciu, 'The Commission's roadmap for digital regulation: updating the EU digital rulebook and regulating the platforms having a gatekeeper position' (5 June 2020) EU Law Live eulawlive.com.

services.[13] While it could be argued that the threat posed by terrorism may entail a derogation, particularly in cases of online public incitement that, as such, require the promptest response, art. 3 of the eCommerce Directive considers that even in cases of urgency the proceeding State has an obligation to notify the Commission and the Member State in which the server is based of any restriction posed to its freedom to provide information services.[14] Moreover, the Commission may even act on this notification by requesting the proceeding Member State to terminate any measure adopted against the services based in another State if they are deemed to be in contrast with European law.

Directive 2017/541/EU sets its main focus on substantive definitions concerning the elements of the crimes therein punished, including the attempt to commit terrorism related acts or the conducts of aiding, abetting or inciting to terrorism (art. 14). The Directive goes as far as imposing Member States a framework of penalties[15] and mitigating circumstances (art. 16) to be handed to those convicted of terrorist crimes, in accordance with the definitions provided by arts 3 and 4.

Moreover, art. 19 provides States with an important procedural disposition concerning the establishment of jurisdiction over terrorist offences. It is to be noted that, along with traditional criteria based on either territorial or personal requirements,[16] this provision allows States to extend their jurisdiction over terrorist crimes committed "in the territory of another Member State".[17] It should be stressed that the European legislator has already envisaged the possibility of a conflict of jurisdiction between Member States willing to prosecute an individual on the same factual basis for alleged terrorist

[13] Restrictions to the freedom to provide information services from another Member States are generally prohibited by art. 3(2). Any derogating measure shall meet the following requirements (para. 4): *i)* necessity, for reasons of public policy, protection of public health, public security or protection of consumers; *ii)* specificity, targeting only the service which prejudices or constitutes a serious and grave threat to the objects of protection; and *iii)* proportionality. The proceeding State shall first comply with some procedural obligations, before adopting any restrictive measure: *i)* ask the target Member State to remedy to its shortcomings and proceed only if such measures were either inadequate or not implemented; *ii)* consequently, notify the Commission and the target Member State of the intention to adopt restrictive measures.

[14] Art. 3(5) and (6) of the Directive 2000/31 cit.

[15] Art. 15 of the Directive 2017/541/EU cit., while encouraging States to adopt "effective, proportionate and dissuasive criminal penalties" (para. 1), also requires them to adapt their national legislation to grave penalties by stating that the maximum sentences shall not be less than the years of conviction therein provided in relation with the specific conducts of arts 3 and 4(2) and (3).

[16] As established by art. 19(1) of the Directive 2017/541/EU cit., those criteria are: "(a) the offence is committed in whole or in part in its territory; (b) the offence is committed on board a vessel flying its flag or an aircraft registered there; (c) the offender is one of its nationals or residents; (d) the offence is committed for the benefit of a legal person established in its territory; (e) the offence is committed against the institutions or people of the Member State in question or against an institution, body, office or agency of the Union based in that Member State".

[17] Art. 19(1) and (2) of the Directive 2017/541/EU cit.

crimes. Indeed, in the event of a disagreement among the proceeding States, they may request Eurojust to coordinate the action of all the domestic authorities involved.[18] As it will be further addressed in the following paragraphs, it is clear that such provision entails the national authorities' willingness to cooperate under the guidance offered by Eurojust, in a field where a swift, coordinated response to a grave threat as that posed by terrorism is crucial. Thus, the Commission's proposal to extend the EPPO's competences to transnational terrorist crimes, that would reduce the margin of dependence on the States voluntariness to cooperate in favour of binding obligations, is to be received with interest.[19]

Building on the framework created by Directive 2017/541/EU, the Commission adopted a Proposal for a Regulation concerning specifically the dissemination of terrorist content online,[20] which was first presented at the European Council held in Salzburg in September 2018 and is, at the time of writing, pending before the Council after being approved by the European Parliament in its first reading in April 2019. The Proposal takes notice of the frequent abuses of the internet by terrorists both in facilitating the organisation and perpetration of attacks and in inciting and recruiting supporters. Thus, with a view to encourage platforms to protect the users from access to such content and tackle the arising cybersecurity issues, the future Regulation addresses both States and hosting providers that have a substantial connection to Member States, which may be determined by either the establishment of the hosting provider, a significant number of users within at least one Member State or the targeting of activities towards at least one Member State.[21]

The Commission has indeed regarded the duty to engage in a systematic supervision over potential terrorist content for companies operating in this business as fairly balanced. The Proposal operated a restriction compared to the previous Recommendation 2018/334, which in turn promoted the adoption of general minimum standards of protection against all kinds of online illicit material. The exclusion of a Proposal contain-

[18] Art. 19(3) of the Directive 2017/541/EU cit. The same article also provides both States and Eurojust with a list of criteria that shall be taken into account in determining the authority having jurisdiction: *i)* the State in which the crime was committed; *ii)* the one of nationality or residence of the offender; *iii)* the country of origin of the victim; or *iv)* the State in which the offender is arrested.

[19] See *infra* section III.

[20] Commission Proposal for a Regulation 2018/640 cit. For some critical remarks, see M Scheinin, 'The EU Regulation on Terrorist Content: An Emperor without Clothes' (30 January 2019) Verfassungsblog verfassungsblog.de; JH Jeppesen and L Blanco, 'Terrorist Content Regulation: MEPs Should Support IMCO and CULT Committees Proposals' (25 January 2019) Center for Democracy & Technology www.cdt.org; K Ramešová, 'Public Provocation to Commit a Terrorist Offence: Balancing Between the Liberties and the Security' (2020) Masaryk University Journal of Law and Technology 137 ff. The necessity to prevent and suppress terrorist conducts perpetrated through the Internet, as well as to further cooperate with private entities to reach this objective, was also addressed in the ACP-EU Joint Parliamentary Assembly Resolution 018/C 415/04 of 15 November 2018 on the urgency of new measures to fight international terrorism, para. 12.

[21] Art. 2(1) n. 3 of Proposal for a Regulation 2018/640 cit.

ing a generalised obligation upon hosting providers to prevent the dissemination of any illicit content online (*e.g*. regarding child pornography or copyright infringements) appears to be a sensible approach, considering that the digital platforms' technological upgrades may lead to unbearable hardships on smaller to medium businesses.[22]

The Proposal for a Regulation, that imposes on hosting providers to remove such illegal material regardless of any order issued by competent authorities, grants them a wide margin of appreciation in the evaluation of which content constitutes terrorist propaganda. While hosting providers should rely on the useful framework of definitions offered by Directive 2017/541/EU, those provisions lack sufficient clarity to be applied directly by private entities. Furthermore, in conformity with the Directive, Member States are entitled to determine autonomously the means by which they can guarantee an immediate elimination of said content: this approach may entail a strong fragmentation as to the measures adopted and frustrates the clear intention of harmonisation of national legislations in this field.[23] Nonetheless, art. 18 of the Proposal requires States to establish a set of effective, proportionate and dissuasive penalties in the event that digital platforms act in violation of the forthcoming Regulation, which may add up to "4 per cent of the hosting service provider's global turnover of the last business year" in case of a systematic lack of compliance with the obligations incumbent upon them.[24]

Moreover, art. 6 requests hosting providers to take proactive measures to prevent the dissemination of terrorist material, both through automated tools and human-based review, insofar as such tools are compatible with the principle of proportionality, in light of "the fundamental importance of the freedom of expression and information in an open and democratic society".

States are however required to monitor if hosting providers comply with this preventive requirement by also respecting art. 15 of the eCommerce Directive, according to which they may not impose on providers any general obligation to monitor information therein stored.[25] While no potentially binding part of the proposed Regulation offers an

[22] It is to be noted however that the Recommendation dedicated a separate section to terrorism, urging States to provide public authorities with "the capability and sufficient resources to effectively detect and identify terrorist content and to submit referrals to the hosting service providers concerned, in particular through national internet referral units and in cooperation with the EU Internet Referral Unit at Europol" (art. 32 of the Commission Recommendation (EU) 2018/334 cit.).

[23] Similarly, this was observed for the case of the implementation of Directive 2017/1371/EU ("PIF Directive", see *infra* section III) in V Mitsilegas and F Giuffrida, 'Raising the bar? Thoughts on the establishment of the European Public Prosecutor's Office' (30 November 2017) Centre for European Policy Studies – Policy Insights www.ceps.eu 8-9.

[24] Arts 18(2) and (4) of Proposal for a Regulation 2018/640 cit. Factors that shall be taken into account by the competent authorities in handing these sanctions include, *inter alia*: "a) the nature, gravity, and duration of the breach; b) the intentional or negligent character of the breach; c) previous breaches by the legal person held responsible; d) the financial strength of the legal person held liable; e) the level of cooperation of the hosting service provider with the competent authorities" art. 18(3).

[25] Art. 15(1) of the Directive 2000/31/EC cit.

effective coordination among these provisions, Recital 19 admits the possibility of derogating from art. 15 of the eCommerce Directive in cases where the public authority recognises "overriding public security reasons" by adopting "certain specific, targeted measures" for a hosting provider. Consequently, two scenarios may concretely occur: either *i)* public authorities find those risks to be *ex ante* subsistent and impose a general obligation of surveillance upon the digital platforms, violating as an effect art. 15 of the eCommerce Directive; or *ii)* such risks materialise into public terrorist content and frustrate the preventive scope of the proposed Regulation.[26]

III. The Commission's proposal on the extension of the EPPO's competence to terrorist conducts

With the view of starting a debate on the potential extension of the EPPO's competences to transnational terrorist crimes, the Commission provided the European Council meeting held in Salzburg in September 2018 with a Communication constituting an initiative on the subject, adopted the same day as the abovementioned Proposal for a Regulation 2018/640.[27]

Indeed, the Commission has recognised that "the Union lacks a European level of prosecution in this area encompassing all steps starting from investigating, prosecuting and ending with bringing to judgement cross-border terrorist crimes" and, as a consequence, "gaps in investigations and prosecutions in one Member State may lead to casualties or risks in another one or in the Union as a whole".[28] In line with the agenda introduced by Junker's Commission, that focused largely on the protection of the European security against threats to be faced unitedly by all Member States, the 2018 Communication builds on the framework created mainly by Directive 2017/541/EU,[29] but al-

[26] Significantly, the CJEU has recently observed, in a preliminary ruling concerning art. 15(1) of the eCommerce Directive, that "[g]iven that a social network facilitates the swift flow of information stored by the host provider between its different users, there is a genuine risk that information which was held to be illegal is subsequently reproduced and shared by another user of that network" (see case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:821 para. 36).

[27] It shall be noted that during the 2018 Salzburg European Council, as well as in the informal meeting held in Sibiu in May 2019, the Commission's proposal has not been taken into account, although President Juncker had clearly addressed the issue of strengthening security within the European borders as a priority in the Commission's agenda, as already stated in the 2017 State of Union – thus before the Regulation on the establishment of the EPPO was even adopted – also with a view of reaching a "more united and more democratic Union by 2025" (Communication on the extension of the EPPO's competences cit. 1).

[28] 2018 Communication on the extension of the EPPO's competences cit. 3.

[29] Indeed, as already considered *supra* (section II), Directive 2017/541/EU represents a comprehensive discipline on terrorism: similarly to a national criminal code, it establishes specific definitions of the conducts and all elements of crime, including strict indications on the sanctions that States shall apply to those found guilty.

so reserves attention to the subsequent question of tackling terrorist crimes perpetrated online.

While potentially acting beyond the limits imposed by art. 83(1) TFEU, which allows the EU to "establish *minimum* rules concerning the definition of criminal offences and sanctions",[30] the Directive certainly paves the way for a procedural regulation on the subject as well. Notably, the very same pattern was followed by Directive 2017/1371/EU ("PIF Directive"),[31] which provides a complete framework for financial crimes (corruption, fraud, misappropriation, money laundering) and constitutes the only substantive basis for the competence of the EPPO.[32]

Preliminarily, it must be stressed that any extension of the EPPO's competences entails a prior amendment to the Treaty by means of a simplified procedure. Pursuant to art. 86(4) TFEU, the EPPO's competences may be extended to crimes other than those affecting the financial interests of the Union with a transnational dimension, by a decision adopted unanimously by the European Council,[33] with the prior consent of the European Parliament and following a consultation with the Council.

Nonetheless, as noticed in its 2018 Communication, no element in the wording of art. 86 TFEU precludes the Commission from forwarding an initiative on the subject to the European Council.[34] Indeed, the institution appears to be already in the proper position to submit a proposal on the extension of the EPPO's competence, given both the 2018 Communication and the abovementioned acts on terrorism previously adopted. Furthermore, this confirms that the prevention and suppression of these crimes constitutes a sensitive matter in the Commission's agenda.

In any event, following the TFEU amendment, the Commission certainly has to present a "legislative proposal to amend Regulation (EU) 2017/1939 so as to grant the competence to the EPPO and introduce any possible adjustment that might be required for the EPPO's effective activities in investigating and prosecuting terrorism".[35] This shall

[30] Art. 83(1) TFEU (emphasis added). An overview on the current debate on the definition of "minimum rules" is provided in M Kettunen, *Legitimizing European Criminal Law: Justifications and Restrictions* (Springer and Giappichelli 2020) 141 ff.

[31] Directive 2017/1371/EU of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law; D Vilas Álvarez, 'The Material Competence of the European Public Prosecutor's Office' in L Bachmaier Winter (ed.), *The European Public Prosecutor's Office: The Challenge Ahead* (Springer 2018) 25 ff.

[32] The potential extension of the EPPO's competence to terrorist crimes, in addition to those considered by the PIF Directive, has been regarded as "highly welcome, because it will address the concerns voiced over the principle of proportionality", not least because the EPPO appears to be a far too costly mechanism to protect the EU budget alone in F De Angelis, 'The European Public Prosecutor's Office (EPPO): Past, Present and Future' (2019) EUCrim eucrim.eu 275.

[33] Thus, an extension of competences shall be approved not only by those States participating in the EPPO's enhanced cooperation, but by all Members of the European Union.

[34] 2018 Communication on the extension of the EPPO's competences cit. 4-5.

[35] *Ibid*.

include a definition of both the personal and territorial scope of application of the EPPO's competence, an assessment on whether to restrict its intervention only to cases exceeding a certain threshold of gravity,[36] as well as a clear definition of the investigative powers and tools that may be employed and of the principles of jurisdiction to be applied by the EPPO and Member States.

The justifications that led the Commission to adopt the Communication can be divided into three main arguments.

First, there is a significant fragmentation in investigating terrorism related crimes. Although Eurojust[37] and Europol[38] have successfully led several States' investigations in such field, every result requires the previous voluntary agreement among the interested Member States. Indeed, both Europol and Eurojust lack a specific power to compel the competent national authorities to act by investigating or prosecuting an alleged case of terrorism. This entails two main negative effects: *i)* a risk of conflict of jurisdiction; and *ii)* an insufficient response due to the unawareness of the potential presence of a criminal cell operating over more than one Member State, also through the inter-

[36] See *infra* for a consideration on whether such threshold may be concretely identified and linked to financial damages.

[37] According to art. 85(1) TFEU, "Eurojust's mission shall be to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States or requiring a prosecution on common bases, on the basis of operations conducted and information supplied by the Member States' authorities and by Europol. In this context, the European Parliament and the Council, by means of regulations adopted in accordance with the ordinary legislative procedure, shall determine Eurojust's structure, operation, field of action and tasks. These tasks may include: (a) the initiation of criminal investigations, as well as proposing the initiation of prosecutions conducted by competent national authorities, particularly those relating to offences against the financial interests of the Union; (b) the coordination of investigations and prosecutions referred to in point (a); (c) the strengthening of judicial cooperation, including by resolution of conflicts of jurisdiction and by close cooperation with the European Judicial Network [...]". See also the recent Regulation (EU) 1727/2018 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust) and replacing and repealing Council Decision 2002/187/JHA, entered into force on 12 December 2019. For an overview on Eurojust's functioning see G De Amicis and RE Kostoris, 'Vertical Cooperation' in RE Kostoris (ed.), *Handbook of European Criminal Procedure* (Springer 2018) 223 ff.

[38] According to art. 88 TFEU, "1. Europol's mission shall be to support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy. 2. The European Parliament and the Council, by means of regulations adopted in accordance with the ordinary legislative procedure, shall determine Europol's structure, operation, field of action and tasks. These tasks may include: a) the collection, storage, processing, analysis and exchange of information, in particular that forwarded by the authorities of the Member States or third countries or bodies; b) the coordination, organisation and implementation of investigative and operational action carried out jointly with the Member States' competent authorities or in the context of joint investigative teams, where appropriate in liaison with Eurojust [...]". For an overview on Europol's functioning see G De Amicis and RE Kostoris, 'Vertical Cooperation' cit. 211 ff.

net. As for the first point, it is quite common that victims of terrorist attacks are of two or more different nationalities. Consequently, prosecutions may legitimately be initiated by a plurality of States, thus giving rise to parallel proceedings creating a situation of *bis in idem*. As for the second one, the inadequacy of cooperation may reasonably result in singular prosecutions and convictions, with no perception of more subtle or sophisticated conducts carried out by groups, potentially leaving those persons coordinating or even in charge of criminal cells across Europe unscathed.[39]

Second, the swiftness in the exchange of relevant information among national authorities or between those authorities and EU agencies is insufficient. As already stressed, Member States are under no duty to cooperate within the instruments provided by both Eurojust and Europol. Thus, there is no binding obligation incumbent upon them to share any information pertaining to the commission of terrorism related crimes. While there is, in principle, no reason to believe that national authorities would necessarily withhold data on the matter that may interest another Member State, the absence of a central body which can control such information still inevitably causes a slowdown in sharing findings that could be vital to ensure the prevention of terrorism.

Third, the lack of common admissibility criteria of collecting and sharing evidence entails the concrete risk of an improper use of sensitive information. In the event that information is indeed shared by States with one another, the gathering of proof, particularly for what concerns circumstantial evidence (*e.g.*, surveillance results, witness statements, intercepts), does not necessarily follow similar practices, which in turn carries the risk of evidence that may be deemed as inadmissible in proceedings before national courts of other Member States.

According to the Commission, all these questions cannot find an adequate answer within the existing framework. While the contribution so far provided by European agencies has been meaningful in order to tackle main terrorist threats,[40] it has become increasingly apparent that the abovementioned factors cause a general weakness in the European system of prevention and suppression of terrorist conducts, particularly for

[39] A clear example of how this particularly problematic question may arise is provided by the Commission itself (2018 Communication on the extension of the EPPO's competences cit. 7-8): a terrorist group may employ agents in more Member States, who operate separately within their country and are tasked with different assignments, that individually considered amount to common offences (*e.g.* forgery of documents, collection of information on targets, purchase of chemical materials and weaponry). As such, the proceeding authorities within one Member State may prosecute those individuals, unaware of the bigger transnational scheme organised by the group leaders, that could easily remain unscathed. However, the scenario therein depicted does not consider the main threat that cannot be contained through a separated approach: terrorism related crimes perpetrated through and facilitated by the internet.

[40] As recognised by the Commission itself: "the added-value of Eurojust and Europol in supporting national authorities and facilitating judicial cooperation on the basis of existing mutual assistance and mutual recognition instruments is crucial" (2018 Communication on the extension of the EPPO's competences cit. 9).

their lack of any power to adopt compulsory measures.[41] Therefore, the extension of the EPPO's competence to such crimes in their transnational dimension can effectively constitute a remedy to the analysed shortcomings,[42] as follows.

First, a comprehensive European effort would bridge the gap among national prosecutions. Through a comprehensive response at the European level and through the work of the European Delegated Prosecutors referring to the central European authority, the EPPO would be empowered with "order[ing] investigations, ensur[ing] the timely collection of further evidence, connect[ing] and prosecut[ing] jointly related cases, and settl[ing] any issues of jurisdiction before bringing a case to court".[43] Indeed, national authorities would be directed by the EPPO, to the point that it may decide that "investigative actions are taken at the time and place where this is most efficient, irrespective of where in the Union these actions must take place".[44] Thus, the risk of incurring in *bis in idem* violations would be reduced to the minimum and, in any event, the European Prosecutor's Office would constitute the best placed authority on dispute resolutions if conflicts of jurisdiction would still persist despite the criteria that shall be established by the amended Regulation on the functioning of the EPPO. Moreover, the EPPO may directly adopt preventative measures, such as the freezing and seizure of assets, and even issue orders of arrest to be executed by national authorities, while also allowing both national and European authorities to detect wider and complex criminal schemes across the Union's territory.

Second, the exchange of information would be appropriate and swift. The EPPO would indeed hold the power to have Member States provide it with data on ongoing investigations, as well as directly order national prosecutors to collect more specific evidence. Furthermore, this would allow domestic authorities to access more easily infor-

[41] However, it has been observed that Member States may prefer to rely on voluntary mechanisms, rather than binding instruments, as counter-terrorism is still considered "a matter of national prerogative, as it very often involves a mix of classical police investigation techniques and surveillance with intelligence, and sometimes counter-insurgency methods, depending on the country", see European Parliamentary Research Service, *Unlocking the potential of the EU Treaties* (May 2020) www.europarl.europa.eu 39. Indeed, Member States may consider that any concrete transfer of power to the EPPO may result in a – so far – undesired harmonisation of national procedures, see JAE Vervaele, 'The European Public Prosecutor's Office (EPPO): Introductory Remarks' in W Geelhoed, LH Leendert and A Meij (eds), *Shifting Perspectives on the European Public Prosecutor's Office* (Springer 2018) 13.

[42] F Trauner, 'EU Internal Security: Countering Threats and/or Respecting Fundamental Rights' (2019) RSCAS Policy Papers 4; A Nato, 'The European Public Prosecutor's Office between counter-terrorism and strengthening of the European citizens' safety' (2016) Civitas Europa 317 ff.

[43] 2018 Communication on the extension of the EPPO's competences cit. 9.

[44] *Ibid*. 10-11.

mation gathered by the European Prosecutor's Office through the creation of new channels interoperable at both levels.[45]

Third, evidence would be shared among Member States on an agreed common standard on the gathering and use of investigative results. In order to request States' cooperation in the exchange of data, the EPPO would necessarily set an acceptable standard of protection of what constitutes sensitive material. This would also facilitate the establishment of best practices under Europol's supervision, particularly in the technological field, thus allowing States to enhance their investigative means and strategies. Therefore, the risk of having evidence collected in other Member States declared inadmissible before national courts would be, once again, minimised.[46]

The delimitation of the area of competence of the EPPO, however, could prove to be a more difficult task for these crimes than for illicit conducts impairing the financial interest of the Union. At the outset, it appears unlikely that a threshold of sufficient gravity could be identified in order to trigger the competence of the EPPO, as opposed to what is already provided by the current Regulation on the establishment of the European Prosecutor's Office, that requires a total damage of not less than 10 million euros in addition to a conduct linked to the territory of at least two Member States. Rather, a more precise definition needs to be found for the element of transnationality, that shall specify whether and to what extent preparatory acts carried out in one State, with the intention to be perpetrated in another Member State, could be deemed as sufficient to entail the EPPO's competence.[47]

The perspective of the implementation of such extension of the EPPO's competence however begs the question of the role that can be envisaged for Europol and Eurojust for the future of the fight against terrorism. As the following section demonstrates, their potential could be adequately employed in countering terrorist content online, in coordination with the EPPO's action.

[45] P Pérez Enciso, 'Exchange and Processing of Information Between the European Public Prosecutor's Office and National Authorities: The Case Management System' in L Bachmaier Winter (ed.), *The European Public Prosecutor's Office: The Challenge Ahead* (Springer 2018) 254 ff.

[46] As already envisaged in European Parliament Resolution P8_TA(2017)0366 of 3 October 2017 on the fight against cybercrime, para. 62: "a common European approach to criminal justice in cyberspace is a matter of priority, as it will improve the enforcement of the rule of law in cyberspace and facilitate the obtaining of e-evidence in criminal proceedings, as well as contributing to making the settlement of cases much speedier than today".

[47] For a similar consideration, see A Juszczak and E Sason, 'Fighting Terrorism through the European Public Prosecutor's Office (EPPO)? What future for the EPPO in the EU's Criminal Policy?' (2019) EUCrim eucrim.eu 70. On the element of transnationality, see also F Giuffrida, 'Cross-Border Crimes and the European Public Prosecutor's Office' (2017) EUCrim eucrim.eu 149 ff.

IV. The persistent role of Eurojust and Europol as crucial cybersecurity and human rights guardians

The answer to the previous question requires more careful considerations as to Eurojust and Europol's role in the field of the prevention and suppression of terrorist conducts.

It appears that the establishment of the EPPO's competence over terrorism related crimes, by admittedly limiting the scope of their action, would conversely enhance their capability as extremely specialised agencies in a more operative-oriented way.[48]

This holds particularly true in light of the recently emended Regulation (EU) 1727/2018 on Eurojust, entered into force in December 2019, that has settled its competence as complementary to that of the EPPO. Indeed, Eurojust must refrain from acting within those fields attributed to the newly established European Prosecutor's Office.[49] Naturally, Eurojust's competence is still in force with regards to those Member States that do not take part in the EPPO's enhanced cooperation or insofar as the European Prosecutor decides not to exercise its competence or directly requests Eurojust to exercise its own.

Three main functions attributed to Eurojust, pursuant to the 2018 Regulation, shall be noticed. Art. 4 tasks the European Agency to "(c) assist in improving cooperation between the competent authorities of Member States, in particular *on the basis of Europol's analyses*; [...] (e) cooperate closely with the EPPO on matters relating to its competence; [...] (g) support and where appropriate participate in the Union *centres of specialised expertise developed by Europol* [...]".[50] Similarly, the 2018 Communication on the extension of the EPPO's competences envisages a close collaboration "with other Union actors, such as Eurojust and Europol, and thus [the EPPO is] strategically placed to enforce the Union's approach to investigating and prosecuting terrorist crimes".[51]

The perspective that can be drawn is that the EPPO shall represent the central authority able to directly enforce instructions upon the domestic prosecutors and to coordinate their joint actions, while Eurojust, with the fundamental support provided by Europol, may continue to tackle illicit conducts relating to terrorism relying on the instruments already created, particularly in the field of online terrorist propaganda.[52] Indeed,

[48] F Spiezia, 'The European Public Prosecutor's Office: How to Implement the Relations with Eurojust?' (2018) EUCrim eucrim.eu 130 ff.

[49] Art. 3(1) of the Regulation (EU) 1727/2018 cit.

[50] Emphasis added.

[51] 2018 Communication on the extension of the EPPO's competences cit. 9.

[52] Notably, computer crimes fall under the competence of Eurojust according to Regulation 1727/2018 cit., Annex I. Furthermore, some scholars have recently argued in favour of the extension of the EPPO's competence to computer crimes, pursuant to art. 83(1) TFEU, considering the opportunity of holding criminally accountable the main internet service providers (*e.g.* Facebook and Google) in cases of failure to ensure an adequate protection of fundamental rights against illicit content published thereon, see L Picotti, 'Diritto penale e tecnologie informatiche: una visione d'insieme' in A Cadoppi, S Canestrari, A Manna and M Papa (a cura di), *Cybercrime* (UTET Giuridica 2019) 89.

the Agency would still hold operating space within such crimes as the EPPO is deliberately not structured to completely replace national prosecutors' competence and allow Member States to maintain a certain degree of autonomy that may be voluntarily transferred over to Eurojust.[53]

Moreover, Eurojust has already implemented some measures intended to prevent and suppress terrorist threats online. In this regard, the European Agency has recently launched, on 1 September 2019, a centralised record (Counter-Terrorism Register – CTR) to collect information on ongoing investigations and proceedings regarding suspects of terrorist attacks.[54] The initiative is based on the principles set by the 2005 Council Decision on the exchange of information concerning terrorism[55] in order to improve the judicial response against such crimes, and was supported by a number of Member States (France, Germany, Spain, Belgium, Italy, Luxembourg and the Netherlands) and the European Commission.

The creation of the CTR proves both the belief, shared by Member States, that a more substantial form of cooperation is needed within the fight against terrorism, and the acknowledgement of the insufficient – even if fundamental – results that can be achieved through the establishment of the Joint Investigation Teams (JITs). Indeed, JITs were first established by Council Framework Decision 2002/465/JHA[56] and may only be constituted by Member States or their national authorities for a specific, predefined objective and a limited time by means of an *ad hoc* agreement, with the support – legal, practical and financial – and under the supervision of Eurojust and, if necessary, of Europol. Significantly, the last meeting of the JITs Network focused on the challenges and opportunities brought forward by cybercrime cases and recognised the inadequacy of traditional instruments (mutual legal assistance, European Investigation Order[57]) in provid-

[53] Indeed, Eurojust's action still largely relies on Member States' willingness to cooperate. This is proved by art. 5(4) of the Regulation 1727/2018 cit., that envisages the repercussions in cases of systematic resistances opposed by States to cooperation: "[a]t the request of a competent authority, or on its own initiative, Eurojust shall issue a written opinion on recurrent refusals or difficulties concerning the execution of requests for, and decisions on, judicial cooperation, including requests and decisions based on instruments giving effect to the principle of mutual recognition, provided that it is not possible to resolve such cases through mutual agreement between the competent national authorities or through the involvement of the national members concerned". See also A Novokmet and Z Vinković, 'Eurojust and EPPO on the Crossroads of their Future Cooperation' (2019) EU and Comparative Law Issues and Challenges Series hrcak.srce.hr 589-590.

[54] Eurojust, 'Supporting Judicial Authority in the Fight Against Terrorism' www.eurojust.europa.eu 1.

[55] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences.

[56] Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigations teams.

[57] The European Investigation Order (EIO) was established by Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. This instrument allows national judicial authorities to issue an order to those of another Member State to carry out specific investigative measures (preservation of evidence, hearings of witnesses or sus-

ing a swift response to cybercrimes, thus proposing a number of conclusions on how to render the JITs more appropriate in order to prevent the perpetration of such crimes.[58]

Thus, Eurojust itself is recognising the opportunity to increase its specialisation in the field of, *inter alia*, cybercrimes. Hence, its interplay with the EPPO on crimes concerning, for instance, online terrorist propaganda, the illicit trade of weaponry on the dark web[59] and the financial exchanges aimed at supporting terrorism, would prove to be fundamental and a most welcomed evolution.

Moreover, by directing its forces towards this sector, rather than being responsible for coordinating national authorities in the fight against terrorism *tout court*, Eurojust could hold a more important role in guiding Europol's efforts and in promoting a stronger cooperation in the operational field. Europol has indeed achieved significant results in the prevention of terrorist conducts through its specialised branch, the European Counter-Terrorism Centre (ECTC), that in turn has created the Internet Referral Units (IRUs), charged with the task of detecting, investigating and referring illicit content of terrorist nature spread through the internet to Member States and hosting providers. IRUs hold a fundamental function not only in the removal of online terrorist content, but also in the identification of the perpetrators of such conducts, which contributes to the attribution of criminal liability within domestic prosecutions.[60] It is worth highlighting that these recent developments targeted against terrorism built on Europol's previous experience with the European Cybercrime Centre (EC3), which has ac-

pects, searches of premises, check of bank and financial data, interception of telecommunications and temporary transfers of persons held in custody) within the jurisdiction of the latter. However, as it has been noticed, the EIO "reflects a one-dimensional approach to cooperation, wherein one party only seeks assistance from another. It does not adequately tackle transnational, interlinked investigations, within the framework of joint teams, networks, EU agencies", see M Luchtman, 'Transnational Law Enforcement Cooperation – Fundamental Rights in European Cooperation in Criminal Matters' (2020) EurJCrimeCrLCrJ 40-41. The lack of a correct coordination between the EIO Directive and the EPPO Regulation has also been underlined in V Mitsilegas and F Giuffrida, 'The European Public Prosecutor's Office and Human Rights' in W Geelhoed, LH Erkelens and AWH Meij (eds), *Shifting Perspectives on the European Public Prosecutor's Office* (Springer 2018) 88-89, inasmuch as the ground for refusal of an EIO for non-compliance with fundamental rights is not recalled in the EPPO discipline.

[58] Eurojust, 'Conclusions on the 15th Annual Meeting of National Experts on Joint Investigation Teams (JITs)' (5-6 June 2019) www.eurojust.europa.eu. For an opposite opinion that considers the JITs' intervention in the field of combating terrorism as sufficient, see MA Arva, 'Frictions on Cross Border Cooperation in Criminal Matters Involving Terrorism Threats' (20 August 2019) Research Association for Interdisciplinary Studies papers.ssrn.com.

[59] Namely, "the encrypted part of the internet accessed using specific software that in themselves are not criminal, such as the Tor browser", see Europol, 'Internet Organised Crime Threat Assessment' (2019) www.europol.europa.eu 44.

[60] See Europol, 'EU Internet Referral Unit Transparency Report of 2018' (20 December 2019) www.europol.europa.eu. The IRUs have already achieved significant results: since their establishment in July 2015 and until December 2018, 83871 decisions for referral were forwarded to Member States and service providers, analysing contents across 179 online platforms.

quired a relevant role in fight against online crimes within the EU since 2013, by also providing Member States with operational and analytical support. Thus, the operational capability of Europol could prove to be of paramount importance, particularly in tackling cybercrimes interrelated with terrorism within the dark web.[61]

The extension of the EPPO's competence to terrorist crimes would then bridge the shortcomings of Eurojust and Europol's action, still largely based on voluntary mechanisms, by creating an obligation of cooperation across all Member States part of the enhanced cooperation, while also benefiting from their fundamental contribution and experience the most threatened field: the internet.

At least one more reason stands in favour of the extension of the EPPO's competence to terrorism and the simultaneous specialisation of Eurojust over terrorist crimes perpetrated through the internet: an increased protection of human rights within the European Union.[62]

It is a well-known fact that States have largely justified the use of mass surveillance and illegal techniques of acquiring evidence in order to strengthen their national security against the ever-growing terrorism threat. In this regard, art. 4(2) TEU, establishes that national security, and the responsibility thereby deriving, shall remain within the exclusive competence of States, as it concerns their essential functioning.[63]

As far as this *Article* is concerned, it suffices to consider that the CJEU's case-law has consistently rejected the use of mass indiscriminate surveillance. Indeed, while the Court has confirmed that individual rights may be sacrificed in the event of a grave threat to public security, which undoubtedly includes terrorism related offences,[64] said

[61] "More coordinated investigation and prevention actions targeting the dark web as a whole are required, demonstrating the ability of law enforcement and deterring those who are using it for illicit activity. An improved real-time information position must be maintained to enable law enforcement efforts to tackle the dark web. The capability will enable the identification, categorisation and analysis through advanced techniques including machine learning and artificial intelligence. An EU-wide framework is required to enable judicial authorities to take the first steps to attribute a case to a country where no initial link is apparent due to anonymity issues, thereby preventing any country from assuming jurisdiction initiating an investigation. Improved coordination and standardisation of undercover online investigations are required to deconflict dark web investigations and address the disparity in capabilities across the EU" (Europol, 'Internet Organised Crime Threat Assessment' cit. 46).

[62] The urge for more adequate considerations over the protection of fundamental rights in the fight against terrorism within the EU has been significantly affirmed in W van Ballegooij and P Bakowski, *The Fight Against Terrorism: Cost of Non-Europe Report* (European Parliamentary Research Service 2018) www.europarl.europa.eu 19 ff.

[63] For a comprehensive reflection on the subject see F Ferraro, 'Brevi note sulla competenza esclusiva degli Stati membri in materia di sicurezza nazionale' in *Temi e questioni di diritto dell'Unione Europea: Scritti offerti a Claudia Morviducci* (Cacucci 2019).

[64] Case C-165/14 *Rendón Marín* ECLI:EU:C:2016:675; case C-304/14 *CS* ECLI:EU:C:2016:674.

notion shall be interpreted restrictively and any derogation must comply with the principle of proportionality.[65]

Thus, the well-established jurisprudence of the CJEU, opened with its leading case *Digital Rights Ireland*,[66] has affirmed that the right to privacy, in its twofold perspective of the respect for private life and the protection of personal data, as enshrined in arts 7 and 8 of the Charter of Fundamental Rights, cannot be restricted to the point of interfering with those rights without a limitation for what is strictly necessary.[67] That is to say that, although the fight against terrorism concerns the general interest of the European population, the use of data surveillance must always meet the requirements of a limited scope of application, and in any case guarantee the right to judicial or administrative review, and provided that the person subjected to such measure is considered to be linked at least indirectly or remotely with the commission of a grave crime.[68]

Moreover, Europol has recently adopted a strong stance against the use of mass surveillance, by defining such measures as "difficult, expensive, not necessarily effective and highly problematic from the perspective of civil liberties and privacy rules".[69] Thus, it appears that there is a trend, starting at the EU level, in favour of the use of targeted tools of investigations when using surveillance on personal data even within the fight against terrorism. This is also confirmed by Directive 2017/541/EU, that provides that the "use of such tools, in accordance with national law, should be targeted and take into account the principle of proportionality and the nature and seriousness of the offences under investigation and should respect the right to the protection of personal data".[70]

Lastly, it appears that evidence, particularly in the field of the suppression of conducts amounting to illicit use of the internet for terrorist purposes, could be collected within the EU through more consistent procedures under the coordination of Eurojust and Europol, thus contributing to a progressive harmonisation of the means of gathering proof that could be used by the EPPO, by also facilitating the issuing of European

[65] Case C-82/16 *K.A.* ECLI:EU:C:2018:308 para. 91.

[66] Joined cases C-293/12 and C-594/12 *Seitlinger and Others* ECLI:EU:C:2014:238.

[67] T Lock, 'Article 8 CFR' in M Kellerbauer, M Klamert and J Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford University Press 2019) 2125: "[t]he question as to whether data retention constitutes a suitable means for fighting serious crime and terrorism remains open. However, in order to be compatible with the requirements of Article 8 CFR, legislation providing for the retention of data cannot be unlimited in its personal scope and must stipulate criteria laying down the circumstances under which data can be retained; furthermore, there must be objective criteria in place determining access and use of that data and clear time limits for its retention. [...] The data subjects concerned must be informed of any access. In addition, the duration of the retention period must be based on objective criteria in order to ensure that it is limited to what is strictly necessary".

[68] *Seitlinger and Others* cit. para. 52 ff.; see also case C-362/14 *Schrems* ECLI:EU:C:2015:650; case C-203/15 *Tele2 Sverige* ECLI:EU:C:2016:970; and, most recently, case C-311/18 *Facebook Ireland and Schrems* ECLI:EU:C:2020:559 para. 168 ff.

[69] Europol, 'The Evolution of Online Terrorist Propaganda' (19 April 2018) www.europol.europa.eu.

[70] Recital 21 of the Directive 2017/541/EU cit.

Investigation Orders. As an immediate consequence, this could lead to a reduction of the cases in which national judicial authorities may recognise impeding reasons to the execution of European Arrest Warrants (EAW) issued by another Member State, claiming the violation of fundamental rights, as the right to privacy, during investigations.

Therefore, the extension of the EPPO's competence to terrorist offences, rather than undermining Eurojust and Europol's role in the fight against organised crimes, could lead to the role as specialised within matters pertaining to cybersecurity and the prevention and suppression of online terrorist conducts, while guaranteeing a high standard of protection *vis-à-vis* those human rights that are constantly impaired, *inter alia*, through the use of mass surveillance.

V. Some conclusive remarks

The extension of the European Public Prosecutor's Office competence to terrorism related crimes can be considered as feasible and advisable in the short future for several reasons.

First, the internet is transnational by nature. Thus, the investigation of online terrorist conducts, which concerns the security of the whole EU geopolitical area, requires a common prosecutorial strategy and the issuing of precise guidelines for hosting providers. This could also grant the EU an autonomous and leading stance in the fight against terrorism on the international stage and strengthen its cooperation with the United Nations' effort on the matter, ultimately benefitting the society as a whole.

Second, the empowerment of the EPPO with a competence on terrorist conducts would grant Eurojust and Europol a more penetrating role within the EU, thus further implementing technologies and best practices through the collaboration of all Member States, facilitating the suppression of terrorist conducts in the most fertile ground for radicalization, training and organization of attacks: namely, the dark web.

Third, a euro-centric competence would allow for more adequate considerations on human rights issues. Indeed, both Europol and the CJEU have reckoned that the use of mass surveillance for investigations bears an inherent risk of human rights violations, that cannot ever be deemed proportionate and strictly necessary in a democratic society. Furthermore, independent prosecutions led by individual Member States may expose defendants to *bis in idem*. Recent CJEU case-law on the EAW clearly demonstrates a trend within the Union of questioning those general principles concerning the prosecution of crimes, thus hindering mutual trust among States.[71] In turn, an extension of the EPPO's competence, in a field marked by well-known violations of those principles,

[71] See for instance the recent preliminary rulings concerning questions on the independence of the public prosecution in Court of Justice, joined cases C-508/18 and C-82/19 PPU *Minister for Justice and Equality v OG and PI* ECLI:EU:C:2019:456; case C-509/18 *Minister for Justice and Equality v PF* ECLI:EU:C:2019:457.

would grant a higher standard of human rights protection and remove obstacles to the execution of EAWs.

While a concrete evaluation of the extension of the EPPO's competences would have been appropriate before the beginning of its work, set to happen by the end of 2020, as terrorist-related crimes could also impair the financial interests of the Union, the Commission itself excluded this possibility in the 2018 Communication on the subject.[72]

Thus, the proper moment to move forward with the present proposal appears to be the end of 2021, as by that time the Commission shall submit a report to the European Parliament and to the Council on the added value brought by Directive 2017/541/EU in the fight against terrorism and "decide on appropriate follow-up actions".[73] Remarkably, in that occasion the Commission shall evaluate "the impact of this Directive on fundamental rights and freedoms, including on non-discrimination, on the rule of law, and on the level of protection and assistance provided to victims of terrorism".[74] This may well include the recognition of whether the Directive constitutes an appropriate and sufficiently detailed substantive framework for the EPPO to build on its investigative jurisdiction, with a view to further developing the way to harmonisation paved by the Directive.

It will certainly be interesting to see whether the Commission will keep considering the security of the EU as one of its priorities for action and put the adequate political pressure on the other institutions. In a moment of such disaggregation, the European Union could find renewed strength in setting far-reaching objectives, demonstrating its peculiar and unique potential not least in the matter of common security.

[72] 2018 Communication on the extension of the EPPO's competences cit.: "[w]ork is on-going to ensure that the EPPO becomes fully operational by the end of 2020. This initiative will not affect the setting up of the EPPO under the existing Regulation (EU) 2017/1939" 4.

[73] Art. 29(2) of the Directive 2017/541/EU cit.

[74] *Ibid*.