ARTICLES

TOWARDS EUROPEAN CRIMINAL PROCEDURAL LAW – SECOND PART
edited by Araceli Turmo

PRIVATE LIFE, PERSONAL DATA PROTECTION AND THE ROLE OF SERVICE PROVIDERS: THE EU E-EVIDENCE PROPOSAL

MARINE CORHAY*

TABLE OF CONTENTS: I. A new framework for the collection of electronic evidence in cross-border cases. – II. Preliminary considerations. – III. Privacy at risk? – IV. Towards a re-allocation of protective functions? – V. Conclusion.

ABSTRACT: In April 2018, the Commission adopted a proposal for the collection of electronic evidence in criminal matters (the so-called e-Evidence Proposal). This proposal pursues the ambition to create an EU-wide legal framework for the collection of electronic evidence in the field of criminal procedure and establishes a new criminal justice paradigm at the EU level: direct cooperation between judicial authorities and service providers. This new type of cross-border cooperation raises important issues, two of which will be addressed in this *Article*. The first issue concerns the impact of this new criminal justice paradigm on the right to protection of personal data and the right to respect for private life. This *Article* will provide an assessment of the options presented by the EU institutions (Commission, Council and European Parliament) to safeguard these rights. The second issue relates to the role of private actors, i.e., service providers. This *Article* will discuss the protective functions assigned to service providers in the Commission's proposal and highlight some of the problematic aspects related to it.

KEYWORDS: electronic evidence – cross-border access to electronic evidence – fundamental rights – law enforcement – data protection – private life.

* PhD Candidate (FRESH Grantee), University of Liège, marine.corhay@uliege.be.

ISSN 2499-8249
doi: 10.15166/2499-8249/477

I. A new framework for the collection of electronic evidence in cross-border cases

Online services, information and communication technologies (ICTs) have revolutionised the way we communicate with one another and the way in which we store, access and share information. Collecting data has proven to be a challenge for law enforcement authorities who have to rely on the cooperation of big global technology companies such as Google, Facebook, Microsoft or Amazon. Over the past two decades, law enforcement authorities have tried, with varying degrees of success, to make these service providers cooperate in cross-border situations in order to avoid resorting to mutual legal assistance procedure. The European Union sensed the great need for a supra-national approach and in June 2016 the Council called on the Commission to take concrete actions to improve cooperation with service providers.[1] This call resulted in a proposal for the collection of electronic evidence in criminal matters (the so-called e-Evidence Proposal or Commission's Proposal) which was issued by the Commission in April 2018. This proposal is composed of two intrinsically linked instruments: a Regulation on European production and preservation orders[2] and a Directive containing harmonised rules on the appointment of legal representatives.[3] The e-evidence proposal pursues the ambition to create an EU-wide legal framework for the collection of e-evidence in the field of criminal procedure that will be based on the principle of mutual recognition and establishes a new criminal justice paradigm at the EU level: direct cooperation between judicial authorities and service providers. This new type of cross-border cooperation raises several questions.[4] It impacts fundamental rights, especially the right to respect for private life and the right to the protection of personal data (part IV). This new criminal justice paradigm also introduces a private actor, the service provider, in the protective framework (part III). Prior to diving into the analysis of these issues, some preliminary considerations on the proposed framework will be exposed (part II).

[1] European Commission Non-paper of 7 December 2016, Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace data.consilium.europa.eu.

[2] Proposal COM(2018) 225 final of the European Commission of 17 April 2018 for a Regulation of the European Parliament and the Council on European production and preservation orders for electronic evidence in criminal matters (hereafter proposed Regulation).

[3] Proposal COM(2018) 226 final of the European Commission of 17 April 2018 for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (hereafter proposed Directive).

[4] See, among others, V Franssen, 'The European Commission's e-Evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?' (12 October 2018) European Law Blog europeanlawblog.eu; M Cole and T Quintel, 'Transborder Access to e-Evidence by Law Enforcement Agencies: A First Comparative View on the Commission's Proposal for a Regulation on European Preservation/Production Order and Accompanying Directive' (University of Luxemburg Law Working Paper Series 10-2018); S Tosza, 'The European Commission's Proposal on Cross-Border Access to e-Evidence' (2018) The European Criminal Law Association's Forum 212; G Robinson, 'The European Commission's e-Evidence Proposal' (2018) European Data Protection Law Review 347.

II. Preliminary considerations

From a law enforcement perspective, data we produce might serve as evidence in a growing number of criminal cases involving all types of crime, not only cybercrime.[5] The borderless nature of the internet means that online services and ICTs may be provided from anywhere in the world; hence data are often processed, transmitted and/or stored by foreign service providers.[6] Therefore, in order to have access to data, law enforcement authorities must rely on the cooperation of these private actors. Contrary to telecom operators, big ICTs companies such as Google, Facebook or Microsoft are not covered by the obligations of telecommunications laws and are located outside the territory of the investigating police and judicial authorities.[7] Law enforcement authorities have resorted to various means to try to make service providers cooperate in cross-border situations in order to avoid resorting to mutual legal assistance procedure, a mechanism that many consider inadequate for the collection of e-evidence.[8] One way is to rely on the voluntary cooperation of service providers, meaning cooperation that is not based on a legal obligation. Some States went further and enacted legislation containing obligations for service providers to comply with law enforcement authorities' requests.[9] In that sense, mandatory cooperation is not new. However, the legal grounds for doing so may be questioned[10]

[5] Proposal COM(2018) 225 final 1 of the European Commission of 17 April 2018 for a Regulation of the European Parliament and the Council on European production and preservation orders for electronic evidence in criminal matters, Explanatory Memorandum (hereafter Explanatory Memorandum); V Franssen, A Berrendorf and M Corhay, 'La collecte transfrontière de preuves numériques en matière pénale. Enjeux et perspectives européennes' (2019) Revue Internationale de Droit Pénal 1; M Stefan and G González Fuster, 'Cross-Border Access to Electronic Data Through Judicial Cooperation in Criminal Matters – State of the Art and Latest Developments in the EU and the US' (2018) CEPS Paper in Liberty and Security in Europe n. 07.

[6] V Franssen, 'The European Commission's e-Evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?' cit.

[7] *Ibid*.

[8] See, among others, S Tosza, 'Cross-Border Gathering of Electronic Evidence: Mutual Legal Assistance, Its Shotcomings and Remedies' in V Franssen and D Flore (eds), Société numérique et droit pénal. Belgique, France, Europe (Larcier-Bruylant 2019) 269; T Christakis, 'E-Evidence in a Nutshell: Developments in 2018, Relations with the CLOUD Act and the Bumpy Road Ahead' (14 January 2019) Cross-border Data Forum www.crossborderdataforum.org; Explanatory Memorandum cit. 7.

[9] See, for instance, arts 46*bis* (production order for traffic and location data) and 88*bis* (production order for identification data) of the Belgian Code of Criminal Procedure and the UK Investigatory Powers Act 2016.

[10] These legislations or practices have substantial extraterritorial effects, affecting the sovereignty of other States. For an analysis of recent Belgian legislation and case-law see V Franssen, 'The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?' (2017) European Data Protection Law Review 534; V Franssen and M Corhay, 'La fin de la saga Skype: les fournisseurs de services étrangers obligés de collaborer avec la justice belge en dépit des possibilités techniques et de leurs obligations en droit étranger, Note sous Cass. 19 février 2019' (2019) Revue de Droit Commercial Belge 1014; P De Hert, C Parlar and J Thumfart, 'Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders: From Yahoo Belgium to Microsoft Ireland' (2018) New Journal of European Criminal Law 326.

and national law, in practice, is not always effective.[11] Besides, the existence of a great variety of national approaches creates fragmentation that generates legal uncertainty for both law enforcement authorities and service providers, as well as conflicting obligations for service providers.[12] The European Union is attempting to remedy that situation with a legal framework for direct cooperation in cross-border situations.[13]

The Commission's proposed Regulation creates binding European Production orders (EPOs) and Preservation orders (EPsOs) for stored data.[14] EPOs enable judicial authorities of the issuing Member State to require a service provider[15] located in another jurisdiction to produce certain data while EPsOs allow for the preservation of data until a subsequent EPO is issued. Both orders are to be addressed to the service provider's legal representative outside the issuing Member State. The proposed Directive obliges European service providers that offer services in more than one Member State, as well as non-European service providers which are active on the EU market, to appoint a legal representative in at least one Member State.[16] The legal representative will function as the EU-wide legal contact person for national competent authorities.[17] The Member State hosting the service provider's legal representative will ensure compliance with orders addressed to the legal representative by the competent authorities of other Member States.[18]

Unlike other forms of cooperation in criminal matters regulated by EU law – like the European arrest warrant (EAW) or the European investigation order (EIO) – which involve the cooperation between judicial authorities of different Member States, the e-Evidence Proposal provides for cooperation between the judicial authorities of one Member State

[11] *Ibid*.

[12] Explanatory Memorandum cit. 2; European Commission Non-paper of May 2017, Improving Cross-Border Access to Electronic Evidence: Findings From the Expert Process and Suggested Way Forward 2.

[13] The e-evidence proposal does not apply to purely national service providers which only have customers in one Member State and non-EU service providers which do not offer services in the EU. See art. 3(2) *a contrario* of the proposed Directive.

[14] Explanatory Memorandum cit. 5. Real-time interception of communication is not covered by the e-evidence proposal.

[15] The proposed Regulation targets specific subcategories of service providers that exceed the scope of application of the traditional telecommunication providers and aims at including internet access services, internet-based services enabling inter-personal communications such as Voice over IP, instant messaging and e-mail services. It also covers cloud and other hosting services and digital marketplaces. See art. 2(3) of the proposed Regulation. Services for which the storage of data is not a defining component are not covered by the proposal. However, providers of internet domain names and IP numbering services are relevant because they "can provide traces allowing for the identification of an individual or entity involved in criminal activity". See Explanatory Memorandum cit. 14.

[16] Art. 3(1) and (2) of the proposed Directive.

[17] V Franssen, 'The European Commission's e-Evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?' cit.

[18] Art. 3(5) of the proposed Directive. To that end, the host Member State will have to enact rules on the basis of which the representative can be held liable for non-compliance. See art. 3(8) of the proposed Directive.

with a service provider (i.e. a private actor) in another Member States, without the involvement of the authorities of the latter Member State, except in case of non-compliance of the service provider. In this framework, service providers will be required to undertake tasks that are usually assigned to the executing State, including the responsibility to assess, in some instances, compliance of the orders with the Charter of Fundamental Rights of the EU (EU Charter). Part IV of this contribution will provide a critical analysis of service providers' newly assigned tasks with regard to fundamental rights.

Production and preservation orders would entail limitations on the right to respect for private life and the right to protection of personal data[19] which are guaranteed by the EU Charter.[20] In addition, personal data may only be processed in accordance with the General Data Protection Regulation (GDPR)[21] and the Law Enforcement Directive (LED).[22] Despite the Commission's claim that the e-Evidence Proposal creates a framework that takes into account the relevant data protection acquis by including sufficient and important safeguards[23] and meets the conditions laid down in art. 52(1) of the EU Charter,[24] the European Parliament and other stakeholders have expressed strong criticisms. The next part (III) of this contribution will analyse the relevant aspects contained in the different versions of the proposed Regulation – the one issued by the Commission in April 2018, the General Approach adopted by the Council of the EU in June 2019[25] and the

[19] Explanatory Memorandum cit. 9. For the purpose of this *Article*, the right to protection of personal data and the right to respect for private life will be considered together. For an analysis of how the two rights collide in the jurisprudence of the Court of Justice of the EU see G González Fuster, 'Fighting for Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection' (2014) Birbeck Law Review 263. For an overview of the differences between the two rights see C Docksey, 'Articles 7 and 8 of the EU Charter: Two Distinct Fundamental Rights' in A Grosjean (ed), *Enjeux europeens et mondiaux de la protection des donnes personnelles* (Larcier 2010) 71.

[20] See arts 7 and 8 of the Charter of Fundamental Rights of the European Union [2012] (hereafter EU Charter).

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter General Data Protection Regulation or GDPR).

[22] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter Law Enforcement Directive).

[23] Explanatory Memorandum cit. 9.

[24] Read as follows: "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

[25] Council of the European Union, General Approach 10206/19 on the Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters (hereafter General Approach).

European Parliament Report issued in December 2020[26] – in order determine what options the EU institutions have put forward to safeguard these rights.

III. Privacy at risk?

The proposed Regulation allows repressive authorities to issue production and preservation orders for stored data which are divided into four categories, namely: subscriber data,[27] access data,[28] transactional data[29] and content data.[30] At a glance, we notice that the Commission distances itself from the traditional data categories – subscriber data, traffic and location data, content data – contained in other instruments, for instance the Cybercrime Convention[31] and previous EU instruments, such as the ePrivacy Directive and the Data Retention Directive.[32] In the proposed Regulation, the category of "traffic and location

[26] European Parliament (LIBE Committee), Report A9-0256/2020 on the Proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters (hereafter European Parliament Report). Prior to the adoption of the Report, on 24 October 2019 the LIBE Committee presented a Draft Report entailing 267 amendments to the Commission's proposed Regulation. See European Parliament (LIBE Committee), Draft Report PR\1191404 on the Proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters (hereafter European Parliament Draft Report). The LIBE Committee's *Rapporteur* is MEP Birgit Sippel.

[27] Art. 2(7) of the proposed Regulation: "data pertaining to: (a) the identity of a subscriber or customer such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone, or email; (b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user".

[28] Art. 2(8) of the proposed Regulation: "data related to the commencement and termination of a user access session to a service, which is strictly necessary for the sole purpose of identifying the user of the service, such as the date and time of use, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the user of a service, data identifying the interface used and the user ID".

[29] Art. 2(9) of the proposed Regulation: "data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, unless such data constitutes access data".

[30] Art. 2(10) of the proposed Regulation: "any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data".

[31] The Convention on Cybercrime refers to subscriber information, traffic data and content data. See Council of Europe, Convention on Cybercrime adopted in Budapest on 23 November 2001, ETS n. 185, arts 1(d), 18(3) and 21.

[32] See art. 2 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereafter ePrivacy Directive); art. 2(2)(a), Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly

data", commonly known as "metadata", is cut up in "access data" and "transactional data".[33] While access to any of these data categories by law enforcement authorities constitutes an interference with the fundamental rights to respect for private life and to the protection of personal data,[34] the Commission considers that the intensity of the impact on fundamental rights varies between different categories of data, in particular between subscriber and access data, on the one hand, and transactional and content data on the other hand.[35] The proposed Regulation entails different levels of protection based on this distinction. According to the Commission, subscriber and access data are less sensitive in nature than transactional and content data and therefore production orders for such data pertain a lower degree of invasiveness hence justifying less strict legal conditions for their production and a larger scope of application.[36] An EPO for subscriber and access data can be issued by a prosecutor or a judge[37] for any type of offence, regardless of its seriousness.[38] Transactional and content data which are considered to be more sensitive are being subject to a higher threshold. An order to produce these categories of data must be issued or validated by a judge[39] in the issuing Member State and is limited to certain categories of offences: criminal offences punishable in the issuing Member State by a maximum custodial sentence of at least three years and a number of harmonised offences "for which evidence will typically be available mostly only in electronic form".[40]

In sum, the Commission's approach is based on the assumption that different levels of protection, based on the sensitive nature of the data and the corresponding degree of invasiveness of the production order, should apply. This approach is meant to respect the principle of proportionality as required by art. 52(1) of the EU Charter and must be assessed with regard to the case-law of the Court of Justice of the EU (Court of Justice). The Court of Justice has issued several landmark decisions regarding the retention of data for law enforcement purposes and its compatibility with arts 7 and 8 of the EU Charter. The analysis of these decisions will be used as guidelines to assess whether the approach adopted by the Commission does indeed comply with the EU Charter. The Court of Justice set the foundations of its jurisprudence in the case of *Digital Rights Ireland*[41] and

available electronic communications services or of public communications networks and amending Directive 2002/58/EC (hereafter Data Retention Directive). This Directive was annulled by the Court of Justice.

[33] V Franssen, 'The European Commission's e-Evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?' cit.

[34] See e.g., case C-207/16 *Ministerio Fiscal* ECLI:EU:C:2018:788 para. 51 (hereafter *Ministerio Fiscal*).

[35] Explanatory Memorandum cit. 14.

[36] *Ibid*. 16; V Franssen, 'The European Commission's e-Evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?' cit.

[37] Art. 4(1) of the proposed Regulation.

[38] *Ibid*. art. 5(3).

[39] *Ibid*. see art. 4(2)(a) and (b).

[40] *Ibid*. art. 5(4); Explanatory Memorandum cit.18.

[41] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd and Seitlinger and Others* ECLI:EU:C:2014:238 (hereafter *Digital Rights Ireland*'. This judgment annulled the data retention directive.

Tele2 Sverige.[42] On the basis of these first rulings, one might be tempted to conclude that, contrary to the Commission's approach, subscriber data and access data are not less sensitive than transactional and content data and therefore accessing these data entails a similar level of interference which may only be justified for the objective of fighting serious crimes. However, as it will be demonstrated, such a conclusion would be insufficiently nuanced.

In *Digital Rights Ireland*, the Court of Justice held that subscriber data, traffic and location data,[43] when taken as a bulk, "may allow very precise conclusions to be drawn concerning the private lives of the persons [...] such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".[44] In *Tele2 Sverige*, the Court of Justice reiterated this conclusion and added that these data provide the means "of establishing a profile of the individuals concerned, information that is *no less sensitive*, having regard to the right to privacy, than the actual content of communications".[45] Concerning access to traffic and location data, in *Tele2 Sverige* the Court of Justice also specifically underlined that access of the competent authorities to these data shall be restricted solely to fighting serious crime.[46] However, the concept of "serious crime" is not defined by EU law[47] and thus it is for national law to determine the conditions under which service providers must produce the requested data.[48] As a consequence, the definition of what constitutes a serious crime may vary depending on the Member State concerned.[49] Therefore the question is whether the minimum threshold of a "maximum sentence of at least three years imprisonment" contained in the proposed Regulation for production orders for transactional and content data corresponds to the definition of the concept of "serious crime". It is doubtful. As emphasized by Prof. Martin Böse in his assessment of the e-Evidence Proposal, the penalty levels in the Member States' national criminal justice systems suggest that it will be rather the

For an analysis see O Lynskey, 'The Data Retention Directive Is Incompatible with the Right to Privacy and Data Protection and Is Invalid in Its Entirety: Digital Rights Ireland' (2014) CMLRev 1789.

[42] Joined cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson and Others* ECLI:EU:C:2016:970 (hereafter *Tele2 Sverige*).

[43] *Digital Rights Ireland* cit. para. 26. The Court refers to the "data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services".

[44] *Ibid*. para. 27.

[45] *Tele2 Sverige* cit. para. 99. Emphasis added.

[46] *Ibid*. para. 125.

[47] The Court notes that in the Data Retention Directive, art. 1(1) simply refers to serious crime as defined by each Member State in its national law. See *Digital Rights Ireland* cit. para. 60.

[48] *Tele2 Sverige* cit. para. 118.

[49] M Böse, 'An Assessment of the Commission's Proposals on Electronic Evidence' (September 2018) www.europarl.europa.eu 40.

exception than the rule that a criminal offence will not meet the minimum threshold for issuing EPOs for transactional and content data.[50] Indeed, contrary to the Commission's claim,[51] the threshold of three-year imprisonment covers petty offences such as simple theft, fraud or assault under the criminal codes of some Member States.[52] For instance, in the Belgian criminal code, a simple theft is punishable by a maximum custodial sentence of five years.[53] Some consider that a requirement that will be met by most offences under national law cannot be considered an adequate threshold for particularly intrusive measures.[54] In a subsequent case, *Ministerio fiscal*, the Provincial Court of Tarragona (Spain) did ask the Court of Justice whether the seriousness of the offence could be determined solely on the basis of the sentence which may be imposed and, if so, what should the minimum threshold be.[55] Unfortunately, the Court of Justice did not answer that question. Yet, this case provides further clarifications with regard to the sensitive nature of data and the corresponding level of interference with fundamental rights. The Court ruled that some subscriber, i.e., data relating to the identity of the user, data are actually less privacy sensitive than traffic and location data.

The Court of Justice combined the two questions asked by the Provincial Court of Tarragona into one: whether access to subscriber data by law enforcement authorities

[50] *Ibid*.

[51] Explanatory Memorandum cit. 17.

[52] European Digital Rights (EDRi), 'Recommendations on Cross-Border Access to Data – Position Paper on the European Commission's Proposal for a Regulation on European Production and Preservations Orders for Electronic Evidence in Criminal Matters' (12 April 2019) edri.org 21, (hereafter EDRi, Position Paper on the European Commission's Proposal for a Regulation on European Production and Preservations Orders for Electronic Evidence in Criminal Matters); M Böse, 'An Assessment of the Commission's Proposals on Electronic Evidence' cit. 40.

[53] Art. 463 of the Belgian Criminal Code for a simple theft, without threat nor violence ("vol commis sans violences ni menaces").

[54] Statement by Judge Marko Bošnjak of the European Court of Human Rights during the European Parliament e-evidence hearing of 27 November 2018 hwww.europarl.europa.eu (2:08:00–2:19:25) (hereafter EP e-evidence hearing); M Böse, 'An Assessment of the Commission's Proposals on Electronic Evidence' cit. 40. Böse considers that in its core, the threshold as defined in art. 5(4) of the proposed Regulation incorporates the exception from the double criminality requirement contained in art. 11(1)(g) of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (hereafter EIO Directive) which read as follows: "Without prejudice to Article 1(4), recognition or execution of an EIO may be refused in the executing State where: the conduct for which the EIO has been issued does not constitute an offence under the law of the executing State, unless it concerns an offence listed within the categories of offences set out in Annex D, as indicated by the issuing authority in the EIO, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years". Emphasis added.

[55] *Ministerio Fiscal* cit. paras 26(2) and 17. The Spanish Criminal Code provides that "serious offences are those which the law punishes with a serious penalty" (art. 13(1)) and "serious penalties shall be: [...] b) imprisonment for a period of more than five years" (art. 33(2)). Art. 579(1) of the Spanish Code of Criminal Procedure provides that access to telephone and telematic communications data which have been retained by service providers may be provided, *inter alia*, for intentional offences punishable by a maximum penalty of at least three years' imprisonment.

entails an interference that is sufficiently serious to entail that access being limited to the objective of fighting serious crime and, if so, by reference to which criteria the seriousness of the offence must be assessed.[56] The case before the Provincial Court of Tarragona concerned a robbery during which the victim was injured and his wallet and mobile phone were stolen.[57] In order to identify the suspects, the law enforcement authorities sought access to the telephone numbers that had been activated with the International Mobile Equipment Identity code (IMEI code) of the stolen mobile phone over a period of 12 days and personal data relating to the identity of the owners or users of the telephone numbers corresponding to the SIM cards activated with the code.[58] The investigating magistrate refused to grant the request on the ground that the measure concerned was limited to serious offences and the facts at issue in the proceedings did not appear to constitute such an offence.[59] The public prosecutor's office appealed against that decision before the Provincial Court of Tarragona.[60] The latter decided to stay the proceedings and to refer two questions to the Court of Justice for a preliminary ruling.[61] The Court of Justice first recalled that access of public authorities to data constitutes an interference with the fundamental rights to respect for private life and to the protection of personal data.[62] The Court then added that "in accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as 'serious'. By contrast, when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally".[63]

Therefore what has to be determined is whether the interference may be regarded as "serious".[64] In this regard, the Court of Justice noted that "the sole purpose of the request at issue in the main proceedings [...] is to identify the owners of SIM cards activated over a period of 12 days with the IMEI code of the stolen mobile phone".[65] The Court found the data concerned "only enables the SIM card or cards activated with the stolen mobile telephone to be linked, during a *specific period*, with the identity of the owners of those SIM cards" and that these data do not allow "precise conclusions to be drawn concerning the private lives of the persons whose data is concerned".[66] Therefore, access to

[56] *Ministerio Fiscal* cit. para. 48.
[57] *Ibid*. para. 19.
[58] *Ibid*. para. 20.
[59] *Ibid*. para. 21.
[60] *Ibid*. para. 22.
[61] *Ibid*. para. 26.
[62] *Ibid*. para. 51.
[63] *Ibid*. paras 56-57.
[64] *Ibid*. para. 58.
[65] *Ibid*. para. 59.
[66] *Ibid*. para. 60. Emphasis added.

these data "cannot be defined as 'serious' interference with the fundamental rights of the persons whose data is concerned".[67] As a consequence, "the interference that access to such data entails is therefore capable of being justified by the objective of preventing, detecting and prosecuting 'criminal offences' generally, *without being necessary that those offences be defined as 'serious'".*[68] In sum, the Court concluded that the interference with fundamental rights caused by law enforcement authorities' access to data relating to the identity of the user – which include data such as surnames, fornames and addresses – is not sufficiently serious to entail that such access must be limited to the objective of fighting serious crimes.[69]

Applying this reasoning to the proposed Regulation would imply that an EPO for subscriber data, at least with regard to those listed in art. 2(7)(a) of the proposed Regulation, because it entails an interference that is not deemed serious, is not restricted to serious crimes.[70] May the same conclusion be reached for access data? The Commission considers that access data, as defined in the proposed Regulation, pursue the same objective as subscriber data, i.e. to identify the user, and that the level of interference with fundamental rights is similar.[71] Nevertheless, one may question whether access data are really less sensitive than transactional data, especially taking into account the fact that, as stated above, both categories are traditionally included in the sole category of "traffic and location data" or "metadata".[72] It should also be noted that the definitions of access data and transactional data partly overlap[73] which may create legal uncertainty about the applicable threshold and risk impeding the rightful use of the production orders by law enforcement authorities.[74] Recalling the aforementioned case-law, subscriber data, traffic

[67] *Ibid*. para. 61.

[68] *Ibid*. para. 62. Emphasis added.

[69] *Ibid*. para. 63.

[70] The Chair of the European Data Protection Board, Andrea Jelinek, is of the opinion that "the lowest threshold providing for the possibility for law enforcement authorities to request access to subscriber and access data for any criminal offence builds on an 'a contrario' reading of the case law of the CJEU". European Data Protection Board (EDPB), Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for Electronic Evidence in Criminal Matters of 26 September 2018 edpb.europa.eu 14(art. 70.1.b) (hereafter EDPB, Opinion 23/2018).

[71] Explanatory Memorandum cit. 15.

[72] The European Data Protection Supervisor is of the opinion that "this data category seems artificial and to have as only objective to attach lower requirements to the production of such data, similar to those attached to the production of subscriber data". See European Data Protection Supervisor (EDPS), Opinion 7/2019 on Proposals regarding European Production and Preservation Orders for Electronic Evidence in Criminal Matters of 6 November 2019 edps.europa.eu para. 21 (hereafter EDPS, Opinion 7/2019).

[73] *Ibid*. para. 22.

[74] M Böse, 'An Assessment of the Commission's Proposals on Electronic Evidence' cit. 20; European Parliament (LIBE Committee), 6th Working Document (B) DT\1181408 on the Proposal for a Regulation on European production and preservation orders for electronic evidence in criminal matters – Safeguards and remedies 5 (hereafter EP (LIBE Committee), 6th Working Document (B)).

and location data, taken as a bulk, may allow very precise conclusions to be drawn concerning the private lives of the persons. When these data provide the means of establishing a profile of the individuals concerned, the Court of Justice considers that such data are *no less sensitive*, having regard to the right to privacy, than the actual content of communications.[75] Therefore, when an EPO for subscriber data and access data allows law enforcement authorities to establish a profile of the individual concerned, it may not be justified by the objective of investigating and prosecuting criminal offences generally.

If we were to resume the reasoning of the Court of Justice in the cases analysed above, it can be stated that the principle of proportionality requires that the seriousness of the interference with fundamental rights matches the level of seriousness of the crime.[76] Unfortunately, the notion of serious crime is yet to be defined by the Court but regarding the seriousness of the interference the Court has consistently emphasized that an interference may be characterised as serious when access to data is likely to allow precise conclusions to be drawn by national authorities concerning the private life of the person whose data are concerned by the access. May other criteria be taken into account in order to determine the seriousness of an interference, such as the duration of the period in respect of which the investigative authorities had access to the data? This question was submitted to the Court of Justice by the Supreme Court of Estonia in the *Prokuratuur* case. The case concerned a woman convicted for theft and the use of another person's bank card. Her conviction relied, *inter alia*, on evidence consisting of traffic and location data which were obtained by the public prosecutor from a provider of electronic communication services.[77] Before Estonia's Supreme Court, the woman challenged the admissibility of the evidence arguing that the national rules on data retention and the subsequent use of the retained data were violating art. 15 of ePrivacy Directive.[78] The Supreme Court of Estonia decided to stay the proceedings and referred three questions to the Court of Justice.

The Court of Justice combined the two first questions asked by the referring Court into one:[79] whether access by public authorities to a set of traffic or location data must be confined to procedures and proceedings to combat serious crime, regardless of the length of the period in which access to those data is sought and the quantity and the nature of the

[75] *Digital Rights Ireland* cit. para. 27; *Tele2 Sverige* cit. para. 99.

[76] AG Saugmandsgaard Øe emphasizes that the establishment of a link between the seriousness of the interference found and the seriousness of the reason that could justify the interference is in line with the principle of proportionality. See case C-207/16 *Ministerio Fiscal* ECLI:EU:C:2018:300, opinion of AG Saugmandsgaard Øe, para. 82.

[77] Case C-746/18 *Prokuratuur* ECLI:EU:C:2021:152 para. 17.

[78] *Ibid*. para. 19.

[79] First, the referring court asked whether access to traffic and location data by State authorities constitutes an interference so serious that it must be restricted to the purpose of fighting serious, regardless of the period to which the retained data to which the State authorities have access relate. Second, the Supreme Court of Estonia asked if, in case the amount of data refered to in its first question is not large (both in terms of the type of data and in terms of its temportal extent), the associated access interference could be justified for any crime.

data available in respect of such a period.[80] In the Supreme Court of Estonia's view, the temporal extent of the period covered by the access to the data is an essential factor for assessing the seriousness of the interference,[81] a view validated by Advocate General Pitruzzella in his opinion on the case. The Advocate General recalls that in the case of *Ministerio Fiscal* the duration period covered by the access was 12 days and that:

> "the seriousness of the interference is determined by taking account of the type of data concerned combined *with the duration of the period covered by the access*. These two considerations make it possible to assess whether the criterion determining the seriousness of the interference has been met, that is to say whether access to the data in question is likely to allow precise conclusions to be drawn by the competent national authorities concerning the private life of the person whose data are concerned by the access. In order to build an accurate profile of someone, it is necessary not only that the access concerns several categories of data, such as identification, traffic and location data, but also that the access covers a period long enough to ascertain with sufficient precision the main features of a person's life".[82]

On 2 March 2021, the Court of Justice delivered its judgment and provided further clarifications on the conditions of access to data relating to electronic communications.[83] The Court noted that the Estonian legislation allows public authorities to seek access to traffic and location retained by service providers in relation to any type of criminal offence.[84] The Court recalled that only non-serious interferences with right to respect for private life and the right to protection of personal data may be justified by the objective of fighting crime in general, as pursued by the Estonian legislation in the proceedings concerned.[85] The Court found that public authority's access to a set of traffic or location data is a serious interference with the aforementioned rights "regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such period, when, as in the main proceedings, that set of data is liable to allow precise conclusions to be drawn concerning the private life of the persons concerned".[86] Therefore, when a set of traffic or location data allows precise conclusions to be drawn concerning someone's private, public authority's access to those data must be confined procedures and proceedings to combat serious crime or prevent serious threat to public security.[87]

[80] *Prokuratuur* cit. para. 23.

[81] *Ibid*. para. 22. Emphasis added.

[82] Case C-746/18 *Prokuratuur* ECLI:EU:C:2020:18, opinion of AG Pitruzzella, paras 81 and 82.

[83] For an analysis of this case see S Rovelli, '*Case Prokuratuur* : Proportionality and the Independence of Authorities in Data Retention' European Papers (European Forum Insight of 11 June 2021) www.europeanpapers.eu 199.

[84] *Prokuratuur* cit. para. 28.

[85] *Ibid*. para. 33.

[86] *Ibid*. para. 39.

[87] *Ibid*. para. 45.

The Court of Justice also confirmed that data relating to the civil identity of users, can be retained and accessed for the purpose of combating crime in general given that, as previously ruled, the interference entailed by a measure relating to these data cannot be classified as serious.[88] In *Prokuratuur* case, the Court makes multiple references to two of its judgment issued in October 2020 – *Privacy International*[89] and *La Quadrature du Net and Others*[90] –, two additional landmark cases on data retention. While it is beyond the scope of this *Article* to analyse these rulings, they are worth mentioning, especially *La Quadrature du Net*, as they provide relevant precisions. In *La Quadrature du Net and Others*, the Court of Justice implicitly and most interestingly makes a subtle reference to the new category of access data proposed by the Commission in its Proposal. In its judgement the Court of Justice found that the ePrivacy Directive allows the general and indiscriminate retention of IP addresses of the sources of a communication in relation to email and internet telephony but only "for a period limited to what is strictly necessary, for the objective of fighting serious crime and preventing serious threats to public security".[91]

Finally, it is important to emphasize that the Court of Justice jurisprudence was rendered in the context of the Data Retention Directive and national laws which imposed general and indiscriminate data retention obligations to service providers. By contrast, EPOs and EPsOs would only be issued to access data in the context of specific proceedings and for a specific period of time. Some are of the opinion that the jurisprudence of the Court makes too little distinction between data retention and subsequent access.[92] Others, such as Advocate General Saugmandsgaard Øe, consider that access to personal data does not present fewer risks for fundamental rights. On the contrary, "danger might even be considered to be greater, in that access to retained data gives concrete form to the potentially harmful use that might be made of the data".[93] In *Prokuratuur* case, the Court stated that access may be justified only by the public interest objective for which service providers were ordered to retain the data.[94] In other words, if the retention of traffic and location can only be justified by the objective of fighting serious crime so does the access to such data. This finding is not without consequence for EPOs and EPsOs. Concerning preservation orders, the proposed Regulation provides that these orders can be issued for all criminal offences and for all categories of data.[95] To the extent that EPsOs

[88] *Ibid*. para. 34.

[89] Case C-623/17 *Privacy International* ECLI:EU:C:2020:790.

[90] Joined cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791.

[91] *La Quadrature du Net and Others* cit. para. 168.

[92] See F Coudert and F Verbruggen, 'Conservation des données de communications électroniques en Belgique: un juste équilibre?' in V Franssen and D Flore (eds), *Société numérique et droit pénal – Belgique, France, Europe* (Larcier-Bruylant 2019) 245; F Verbruggen, S Royer and H Severijns, 'Reconsidering the Blanket Data-Retention-Taboo, for Human Rights' Sake?' (1st October 2018) European Law blog europeanlawblog.eu.

[93] See *Ministerio fiscal*, opinion of AG Saugmandsgaard Øe, cit. para. 38.

[94] *Prokuratuur* cit. para. 31.

[95] Art. 6(2) and (3)(d) of the proposed Regulation.

will allow for the retention of data, a comparison can be drawn with the data retention measures analysed in the jurisprudence of the Court of Justice with the difference being that EPsOs will concern specific proceedings and relate to a specific set of data. It can therefore be argued that EPsOs qualify as targeted measures.[96] While the Court consistently stated that "general and indiscriminate" retention of traffic and location data was precluded by the Charter even for the purpose of fighting serious crime,[97] in its judgements of October 2020, the Court leaves the door open to targeted data retention measures for traffic and location data.[98]

Nevertheless, preservation orders have also raised concerns with regard to the principles for the processing of personal data. Since all four categories of data detailed in the proposed Regulation do contain information related to an identified or identifiable natural person they are considered as personal data and are therefore covered by the safeguards under the EU data protection law.[99] The General Data Protection Regulation and the Law Enforcement Directive provide that several principles must be respected when personal data are processed by private companies and law enforcement authorities.[100] In the proposed Regulation, the principles of data minimisation and storage limitation are at stake. The proposed Regulation does not guarantee that the preservation of the data will be limited to what is necessary to produce.[101] The proposed Regulation stipulates that data must be preserved for a period of sixty days, unless the issuing authority confirms that a request for production has been launched.[102] Once a production order has been issued, data must be preserved as long as necessary in order to be produced once the subsequent request for production is served to the service provider.[103] In case the preservation would no longer be necessary, the issuing authority shall inform the service provider "without undue delay".[104]

What the Commission's Proposal does not indicate, nor does the General Approach or the Draft Report, is what instrument – the GDPR or the Law Enforcement Directive – should apply between private companies and law enforcement authorities when the latter seek access to data stored by the former for purposes other than criminal justice. The question

[96] Besides AG Saugmandsgaard Øe, in his opinion in *Ministerio fiscal*, acknowledged that the requested access did not constitute a serious intereference and one of the reasons behind this assertion was that the transmission of the data was sought as a targeted measure, i.e., access by the competent authorities and for the purposes of a criminal investigation. See *Ministerio Fiscal*, opinion of AG Saugmandsgaard Øe cit. para. 37.

[97] See *Tele2* cit. para. 112; *Prokuratuur* cit. para. 30; *La Quadrature du Net and Others* cit. para. 168.

[98] See *La Quadrature du Net and Others* cit. para. 168. For an analysis of *La Quadrature du Net and Others* and *Privacy International* see J Sajfert 'Bulk Data Interception/retention Judgments of the CJEU – A Victory and a Defeat for Privacy' (26 October 2020) European Law Blog europeanlawblog.eu.

[99] EDPB, Opinion 23/2018 cit. 12; art. 4(1) General Data Protection Regulation.

[100] See art. 5(1) General Data Protection Regulation cit. and art. 4(1) Law Enforcement Directive cit.

[101] EDPB, Opinion 23/2018 cit. 6.

[102] Art. 10(1) of the proposed Regulation.

[103] *Ibid*. art. 10(2).

[104] *Ibid*. art. 10(3).

is not purely theoretical.[105] Even though the GDPR and the Law Enforcement Directive contain similar principles for the processing of personal data those instruments also contain some very distinct features that are not without consequence for data subjects. For instance, the principle of purpose limitation which constitutes a safeguard against the misuse or abuse of personal data is given a different interpretation in a law enforcement context.[106] In *La Quadrature du Net and Others* and *Privacy International*, the Court of Justice found that data processing carried out by individuals (e.g. service providers) for, *inter alia*, law enforcement purposes falls within the scope of the General Data Protection Regulation. While when Member States do not impose processing obligations on private actors the processing is regulated by national law, subject to the application of the Law Enforcement Directive.[107] However, the reasoning of the Court on that matter is debatable.[108]

Regarding the issuing authorities, the Court of Justice has ruled that access to retained data "should, as a general rule, except in cases of validly established urgency, be subject to prior review carried out either by a court or by an independent administrative body [...] following a reasoned request of competent national authorities submitted within the framework of procedures of prevention, detection or criminal prosecution".[109] The proposed Regulation opens the possibility for public prosecutors to issue or authorise the issuance of production orders for subscriber data and access data[110] hence what has to be determined is whether a public prosecutor may be considered as an independent administrative body. In recent joined cases, the Court found that French, Swedish and Belgian public prosecutor's offices where sufficiently independent from the executive hence satisfying the requirements for issuing a European arrest warrant.[111] Following that decision, one might be tempted to reach the conclusion that a public prosecutor could meet the threshold of independence required in the context of data retention. However, the Court has ruled otherwise. In the aforementioned case of *Prokuratuur*, the third question asked by the Supreme Court of Estonia was whether the public prosecutor's office of Estonia is an

[105] Regarding information sharing between private actors and public authorities see N Purtova, 'Between the GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnership'(2018) International Data Privacy Law 52.

[106] See C Jasserand, 'Subsequent Use of GDPR Data for Law Enforcement Purpose – The Forgotten Principle of Purpose Limitation?'(2018) European Data Protection Law Review 152; C Jasserand, 'Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?' (2018) Computer Law & Security Review 163.

[107] *La Quadrature du Net and Others* cit. para. 103; *Privacy International* cit. paras. 47-48.

[108] See P Vogiatzoglou and J Bergholm, 'Privacy International & La Quadrature du Net: The Latest on Data Retention in the Name of National and Public Pecurity – Part 3' (27 October 2020) CiTiP Blog www.law.kuleuven.be.

[109] *Tele2 Sverige* cit. para. 120; *Digital rights Ireland* cit. para. 62.

[110] Art. 4(1) and (3) of the proposed Regulation.

[111] See case C-625/19 *Openbaar Ministerie (Swedish Public Prosecutor's Office)* ECLI:EU:C:2019:108; joined cases C-566 and C-626/19 *Parquet Général du Grand-Duché du Luxembourg and de Tours* ECLI:EU:C:2019:1077; case C-627/19 *Openbaar Ministerie* (Public Prosecutor, Brussels) ECLI:EU:C:2019:1079.

independent administrative body within the meaning of *Tele2 Sverige*. In other words, the referring court is asking whether the Estonian public prosecutor has the power to authorise access to traffic and location data. In his opinion, Advocate General Pitruzzella recalled that the Court of Justice specific assessment made in that particular context cannot be applied automatically to other areas, such as the protection of personal data.[112] After exposing detailed considerations, he reached the conclusion that the public prosecutor's office of Estonia did not qualify as an independent administrative body because national law provides that the public prosecutor's office "is responsible for directing the pre-trial procedure, whilst also being likely to represent the public prosecution in judicial proceedings."[113] In its judgement, the Court of Justice reiterated that a prior review by a court or by an independent administrative body prior to access to the data is an essential safeguard.[114] The said court or body must be able to strike a fair balance between the needs of the investigation and the rights to protection of personal data and respect for private life of the persons concerned.[115] The Court of Justice declared that the requirement of independence means that the authority must be a third party in relation to the authority which requests access to the data, which is not the case of the Estonian public prosecutor. The Court followed the reasoning of the Advocate General and found that due to its involvement in the conduct of the criminal investigation and its position in the proceedings, the Estonian public prosecutor does not qualify as an independent administrative body.[116]

While the Commission's Proposal was criticised, the General Approach adopted by the Council triggered even harsher criticisms (*see infra*).The Council kept the new data categories introduced by the Commission [117] and extended the scope of application of EPOs and EPsOs. The General Approach provides that orders can be issued in proceedings concerning the execution of a custodial sentence or a detention order of at least four months.[118] Furthermore, "in validly established emergency cases", any other competent authority – meaning other than a judge, a court, an investigating judge or a prosecutor – may issue production orders for subscriber and access data and preservation orders "without prior validation" if these authorities could issue orders in a similar domestic case without validation.[119] In other words, in case of emergency, production orders for subscriber and access data and preservation orders no longer require prior validation by a

[112] *Prokuratuur*, opinion of AG Pitruzzella, cit. para. 104.

[113] *Ibid*. para. 129. His opinion is puzzling. One can legitimately question the reasons justifying that a prosecutor satisfying the requirements for issuing a European arrest warrant, potentially resulting in the deprivation of someone's liberty, would not qualify as an independent administrative body in the area of the protection of personal data.

[114] *Prokuratuur* cit. para. 51.

[115] *Ibid*. para. 52.

[116] *Ibid*. paras 54-55.

[117] See art. 2(7) to (10) of the General Approach cit.

[118] *Ibid*. see arts 5(3), 5(4)(d) (production orders) and 6(2) (preservation orders).

[119] *Ibid*. see art. 4(5) read in conjunction with arts 4(1)(a) and (3)(a).

judge, a court, an investigating judge or a prosecutor when issued by "another competent authority".[120] By doing so, the General Approach further weakened the safeguards for subscriber and access data.

The European Parliament, in its Draft Report, rejected the Commission's data categories[121] and opted to return to the traditional data categories – subscriber data, traffic data and content data – "based on existing EU law and national legislation and in line with Court of Justice case-law".[122] In the Report adopted in December 2020, while the European Parliament sticks to the traditional categories of traffic data and content data,[123] the definition of subscriber data includes an additional type of data compared to the Draft Report. Subscriber data also covers "the type of service provided and the duration of the contract with the service provider, which is strictly necessary for the sole purpose of identifying the user of service".[124] Besides, the Report provides that EPOs may be issued to obtain IP addresses "for the sole purpose of determining the identity of specific persons with a direct link to the specific proceedings" under the same conditions that EPOs for subscriber information.[125] Allowing the issuance of EPOs for such a category of data strongly echoes the recent jurisprudence of the Court of Justice. In *La Quadrature du Net and Others*, the Court of Justice opened to the door to the general and indiscriminate retention of IP addresses for the purpose of, *inter alia*, fighting serious crime.[126] The Court recognized that while IP addresses fall within of the category of traffic data, in relation to email and internet telephony IP addresses of the *source of the communication* is a category of data that is less sensitive than other traffic data.[127] The Court also acknowledged that for criminal offences committed online, IP addresses might be the only means to identify the suspect or perpetrator.[128] In order words, by allowing the general and indiscriminate retention of such data the Court provides law enforcement authorities with a tool to identify unknown individuals suspected of having committed a criminal offence and so does the European Parliament Report. There is, however, a difference between the jurisprudence of the Court and the Report. In the latter, EPOs for IP addresses can be issued for

[120] The article stipulates that the validation must be sought ex-post "without undue delay, at the latest within 48 hours". When such ex-post validation is not granted, the issuing authority must withdraw the order "immediately and shall, in accordance with its national law, either delete any data that was obtained or ensure the data are not used as evidence".

[121] Amendments 91 and 92 of the European Parliament Draft Report cit.

[122] *Ibid*. 147.

[123] See art. 2(8) and (9) of the European Parliament Report cit.

[124] *Ibid*. See art. 2(7).

[125] *Ibid*. See arts 4(1) and 5(3).

[126] See *La Quadrature du Net and Others* cit. para. 155.

[127] *Ibid*. para. 152. Emphasis added. The same reasoning cannot be applied to the IP addresses of the recipient of the communication.

[128] *Ibid*. para. 154.

all criminal offences[129] while in the aforementioned case the Court allowed for the retention of such data, and *a fortiori* subsequent access by state authorities, only for the purpose of fighting serious crime. Nevertheless, as argued earlier, the jurisprudence of the Court concerns data retention and cannot be completely transposed to EPOs and EPsOs. EPOs for IP addresses will be issued in relation to specific proceedings and for a specific period of time hence constituting a targeted measure.

Regarding EPOs for traffic and content data, while the Draft Report raised by two years the threshold to issue such orders,[130] in the end the European Parliament maintained the threshold contained in the Commission's Proposal, i.e., criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least three years.[131] Concerning the issuing authorities, the Report limits the competence of public prosecutors. It provides that EPOs for traffic data and content data may only be issued by a judge, a court or an investigating judge.[132] Public prosecutors may only issue EPsOs and EPOs for subscriber data and IP addresses.[133]

As exposed throughout this part, the Commission's Proposal intends to establish common standards for direct cooperation with service providers in cross-border cases. Nevertheless, Member States will still be required to combine EU rules with national rules on criminal procedure. The new cooperation regime will be regulated by national laws, especially the national laws of the issuing Member State. Indeed, according to art. 5(2) of the proposed Regulation an EPO can only be issued if a similar measure would be available in a comparable domestic case. In other words, the substantive requirements (e.g., threshold, privileges and immunities) for a domestic production order apply accordingly.[134] The Commission's Proposal does not refer to the protection provided by formal and substantive requirements for production orders under the law of the Member State where the service provider is addressed. As a consequence, and in accordance with the principle of mutual recognition, the competent authority of the enforcing Member State must enforce the order even if domestic law provides for a higher standard of protection than the law of the issuing Member State.[135] Therefore, the European Union's ability to maintain the high level of protection granted to the right to respect for private life and to the protection of personal data is crucial in order to overcome the fragmentation of national laws which

[129] Art. 5(3) of the European Parliament Report cit.

[130] Art. 5(4) of the European Parliament Draft Report cit. stipulates that EPOs for these categories "may only be issued for criminal offences punishable in the issuing State by a custodial sentence of a maximum sentence of at least five years". One can ask whether this new threshold could have led to a race to more severe penalties at national level in order to fall within this requirement.

[131] Art. 5(4) of the European Parliament Report cit.

[132] Amendment 106 of the European Parliament Draft Report cit.

[133] Art. 4(1)(a) and (3)(a) of the European Parliament Report cit.

[134] M Böse, 'An Assessment of the Commission's Proposals on Electronic Evidence' cit. 43.

[135] *Ibid*. 39.

may create variable levels of protection among Member States. That said, in some instances, European law may be less strict than the law of the issuing Member State. As previously explained, several authorities are entitled to issue EPOs and EPsOs. In the proposed Regulation while judges, courts and investigating judges may issue both types of orders and for all types of data, public prosecutors may only issue EPsOs and EPOs for subscriber data and access data. Given the fact that a Regulation, and not a directive, will be enacted, Member States will not have the option to restrict the circle of authorities entitled to issue EPOs and EPsOs, by further limiting the power of the public prosecutor for instance.[136] As a result, a prosecutor might be in the position to issue a preservation order at the European level while it would not be possible in a purely domestic context. In this scenario, conditions to issue orders may be stricter for national orders than for European orders which would have the potential to influence national law. States might have been tempted to align their national legislation with (lower) EU standards. The Report does suppress that risk by providing that EPOs and EPsOs may be issued "if it could have been ordered under the same conditions in a similar domestic case".[137]

By way of conclusion, it can be asserted that the EU institutions have different visions on the conditions that should apply to the issuance of EPOs and EPsOs, which offer different levels of protection to the right to protection of personal data and the right to respect for private life. Another highly, if not the most, controversial aspect of the Commission's proposed Regulation concerns the role assigned to service providers.[138] In the framework proposed by the Commission, a private actor will have to assess compliance with the EU Charter – a responsibility which, in principle, lies with Member States and the EU institutions. The following part of this contribution will discuss the protective functions allocated to service providers in the e-Evidence Proposal and highlight some of the problematic aspects related to it. Then, it will present the option chosen by the European Parliament to prevent service providers from becoming legal assessors of fundamental rights.

IV. Towards a re-allocation of protective functions?

The approach chosen by the Commission regarding service providers has been described as a re-allocation of protective functions.[139] In the Commission's proposed Regulation, the legal representative of the service provider is given the role of the "addressee" of

[136] S Tosza, 'The European Commission's Proposal on Cross-Border Access to e-Evidence' cit. 214.

[137] Arts 5(2) and 6(2) of the European Parliament Report cit.

[138] See European Digital Rights (EDRi), 'EU "e-Evidence" Proposals Turn Service Providers into Judicial Authorities' (17 April 2018) edri.org; EuroISPA, 'e-Evidence: EuroISPA Adopts Position Paper' (3 July 2018) www.euroispa.org; Council of Bars and Law Societies of Europe (CCBE), 'Recommendations on the Establishment of International Rules for Cross-Border Access to Electronic Evidence' (28 February 2019) www.ccbe.eu 3, (hereafter CCBE, Recommendations on Cross-Border Access to Electronic Evidence); M Böse, 'An Assessment of the Commission's Proposals on Electronic Evidence' cit. 41.

[139] Expression used by M Böse, 'An Assessment of the Commission's Proposals on Electronic Evidence' cit. 41.

EPOs and EPsOs.[140] In practice, a competent judicial authority in the EU, the issuing authority, will address an order – to preserve or produce data – through a standardised certificate[141] directly to the service provider's legal representative in the EU and the data will be provided directly to the issuing authority.[142] The authorities in the EU Member State where the service provider is addressed will not receive the order and will not be involved in the process except when the service provider refuses to execute an order or does not comply with an order.[143] This is a completely new paradigm. In the sphere of criminal justice, the enforcement of a judicial decision of one Member State in another Member State has always required the intervention of the competent authorities of the Member State where the decision is executed, notwithstanding the principle of mutual recognition. This is the case even for recent instruments such as the EIO Directive.[144]

Because service providers will be the addressee of EPOs and EPsOs, they will bear the responsibility to execute these orders and the Commission's proposed Regulation provides for several grounds of refusal to execute EPOs and grounds to oppose the enforcement of EPOs and EPsOs. Concerning EPOs, art. 9(5), subparagraph 2 of the proposed Regulation stipulates that the addressee, i.e., the service provider's legal representative, may refuse to execute an EPO if it is apparent that it "manifestly violates the Charter" or that it is "manifestly abusive". At that stage, this possibility does not exist for EPsOs. If the service provider does not comply with its obligation, the Member State where it is addressed steps in to enforce the order. During this enforcement process, the service provider may oppose the EPO, but also the EPsO, if it is apparent that it "manifestly violates the Charter" or that it is "manifestly abusive".[145] This is no coincidence that the State where production and preservation orders are executed is called the enforcing State in the proposed Regulation whereas in the EIO Directive the State is called the executing State, different names entail different functions. In the proposed Regulation, the State where the EPO or the EPsO is executed is only assigned a very limited role of review at the enforcing stage[146] which means that this State may only have a say if the service provider refuses to comply with the order.[147] *A contrario*, when the service provider complies with an order, the enforcing State might not even be aware of the existence of the

[140] Art 7(1) of the proposed Regulation. If a designated legal representative does not exist or does not comply with its obligations, the order may be addressed to any establishment of the service provider in the Union. See art. 7(2) to 7(4) of the proposed Regulation.

[141] *Ibid.* art. 8(1).

[142] *Ibid*. art. 9(1).

[143] Explanatory Memorandum cit. 3.

[144] See art. 1(1) EIO Directive cit.

[145] Art. 14(4)(f) and. 14(5)(e) of the proposed Regulation.

[146] See *Ibid*. art. 14(6).

[147] Under art. 14(2) of the proposed Regulation, "the enforcing authority shall without further formalities recognise a European Production Order or European Preservation Order transmitted in accordance with paragraph 1 and shall take the necessary measures for its enforcement, *unless the enforcing authority considers that one of the grounds provided for in paragraphs 4 or 5 apply or that the data concerned is protected*

order, neither will it be able to object. As a consequence, the enforcing State will not be able to exercise its protective functions by refusing to execute orders on human rights' grounds.[148] The protective functions are assigned to the competent authority in the issuing State and the addressee of the order, a private actor.

Several actors have strongly advocated against the curtailing of the role and responsibilities of the Member State where the order is to be executed.[149] Under human rights law, States have the obligation to respect human rights and to ensure these rights to all individuals within its territory.[150] The LIBE Committee's *Rapporteur* stressed that, taking into account the fact that all Member States of the EU are parties to the European Convention on Human Rights (ECHR), they are responsible for the protection of human rights on the territory under their jurisdiction.[151] In this regard, an important aspect should not be overlooked. In the digital world, the State where the order is executed is rarely the State where the person concerned by the order resides.[152] In other words, there may not

by an immunity or privilege under its national law or its disclosure may impact its fundamental interests such as national security and defence". Emphasis added. The issuing State transfers the order to the State where the service provider has its representative (the enforcing State) in order for the latter to take measures to enforce the order.

[148] M Böse, 'An Assessment of the Commission's Proposals on Electronic Evidence' cit. 41. In the context of the European arrest warrant, a refusal to execute for violation of fundamental rights has long been a hard bone of contention. The Framework Decision on the European arrest warrant (EAW) does not include a ground for refusal based on fundamental rights. At first, the Court of Justice leaned towards law-enforcement demands despite fundamental rights considerations. However, more recently, the Court seems to have restored the balance between the protection of fundamental rights and the effectiveness of the instrument by allowing States to refuse the execution of an EAW based on human rights grounds. On this topic see L Mancano, 'A New Hope? The Court of Justice Restores the Balance Between Fundamental Rights Protection and Enforcement Demands in the European Arrest Warrant System' in A Weyembergh and C Brière (eds), *The Needed Balances in EU Criminal Law. Past, Present and Future* (Hart Publishing 2018) 285; J Ouwerkerk, 'Balancing Mutual Trust and Fundamental Rights Protection in the Context of the European Arrest Warrant' (2018) European Journal of Crime, Criminal Law and Criminal Justice 103.

[149] See, for instance, Opinion 23/2018 cit. 17; Opinion 7/2019 cit. para. 42; Recommendations on Cross-Border Access to Electronic Evidence cit. p. 3; European Parliament (LIBE Committee), 3rd Working Document (A) DT\1176298, Execution of EPOC(-PR)s and the role of service providers 4-5, (hereafter EP (LIBE Committee), 3rd Working Document (A)).

[150] See United Nations, International Covenant on Civil and Political Rights of 23 March 1976, art. 2.

[151] EP (LIBE Committee), 3rd Working Document (A) cit. 5; see Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) of the 4 November 1950, art. 1.

[152] See T Christakis, 'Lost in Notification? Protective Logic as Compared to Efficiency in the European Parliament's e-Evidence Draft Report' (7 January 2020) Cross-Border Data Forum www.crossborderdataforum.org. He emphasizes that this is a big difference compared to the physical world where the executing State is often at the same time the affected State. For instance, when State A resorts to mutual legal assistance in order to request from State B an investigative measure that will be executed on its territory (e.g. search and seizure of property), the affected State (State B) is also the executing State. State B can exercise its protective functions and refuse to execute such a request if that State considers that this would violate the human rights of the person present on its territory and targeted by the request.

be a match between the territory of the enforcing State and the territory where the person targeted by the order resides hence some authors[153] and the European Parliament's *Rapporteur* (see *infra*) plead for a notification to the "affected State", meaning the Member State of permanent residence of the affected person.[154] Two questions therefore arise. First, can a Member State rely on EU law to be discharged of its protective functions?[155] In *Matthews v United Kingdom* the European Court of Human Rights (ECtHR) ruled that even after a contracting State transfers part of its sovereignty to an international organisation such as the EU (European Community at the time), its responsibility to protect human rights continues.[156] Subsequently, the European Court developed the *Bosphorus* doctrine. The ECtHR considers that the EU protects fundamental rights in a manner that is at least equivalent to the ECHR and presumes that "a State has not departed from the requirements of the Convention when it does no more than implement legal obligations flowing from its membership".[157] However, this presumption is rebuttable, if "in the circumstances of a particular case, it is considered that the protection of Convention rights was manifestly deficient".[158] During a hearing held by the European Parliament in November 2018, Marko Bošnjak, judge at the ECtHR, recalled that the Court has dealt with mutual recognition in previous cases and "has accepted the presumption of equal protection but if the authorities of the enforcing State are faced with a complaint that the protection of conventional rights has been manifestly deficient and this cannot be remedied by EU law, they cannot refrain from examining the complaint on the ground that they are just applying EU law".[159]

The second question concerns the role of private actors. May a service provider exercise protective functions?[160] As of today, neither the jurisprudence of the European Court nor the jurisprudence of the Court of Justice have ventured into this matter. On the political level, the idea of private actors acting as fundamental rights' assessors is highly

[153] See T Christakis, 'E-Evidence in the EU Parliament: Basic Features of Birgit Sippel's Draft Report'(21 January 2020) European Law Blog europeanlawblog.eu.

[154] Amendment 100 of the Draft Report. However, the affected State will not have the ability to object orders (see *infra*).

[155] This issue was raised by Judge Marko Bošnjak of the European Court of Human Rights during the EP e-evidence hearing.

[156] See ECtHR *Matthews v United Kingdom* App n. 24833/94 [18 February 1999] para. 32.

[157] ECtHR *Bosphorus Hava Yollari v Ireland* App n. 45036/98 [30 June 2005] para. 156.

[158] *Ibid*.

[159] Statement by Judge M Bošnjak, EP e-evidence hearing. It has been stated in *Avotins v Latvia* regarding art. 6 of the Convention and concerned the functioning of the EU system of mutual recognition of judgments in civil and commercial matters. See ECtHR Avotins v Latvia App n. 17502/07 [23 May 2016] para. 116. This jurisprudence was confirmed later on in a number of instances. In the context of the EAW, see ECtHR *Pirozzi v Belgium* App n. 21055/11 [17 April 2018].

[160] It is beyond the scope of this *Article* to determine whether service providers should and could play a role in the protection of fundamental rights. This question will be addressed over the next few years by the present author in her thesis.

contentious. The LIBE Committee, has taken a strong stance against the protective functions assigned to service providers and the corresponding loss of protective functions for the State where the order is to be executed (see *infra*). What can be said so far is that, if the EU institutions were to agree that service providers may play a role in the protection of fundamental rights, the way this role has been shaped in the proposed Regulation is problematic in several respects. Legal and practical considerations will allow us to demonstrate that the proposed Regulation has not given service providers proper means to duly fulfil protective functions.

First of all, the service provider's legal representative will not receive the full order, only a standardized certificate which will contain very limited information regarding the specific case to which an order is linked. This certificate will also not contain the necessity and proportionality analysis related to the order.[161] These two elements alone demonstrate that a human rights assessment will be hardly possible. Furthermore, the order will refer to a foreign legal system, namely the law of the issuing State. One can argue that the criminal provisions on which an order is based may not be sufficiently accessible to the service provider.[162] Even if foreign national laws were to be accessible, it would be unrealistic to expect service providers to have sufficient knowledge of the functioning of each Member State's criminal justice system. In addition, a closer look at the human rights clause displayed in the proposed Regulation reveals that the protective functions delegated to service providers can only be described as limited, if not weak. The human rights clause contained in arts 9(5), 14(4)(f) and 14(5)(e) is limited to "manifest" violations that are "apparent from the sole information contained in the order". The term "manifest" has not been defined and, as previously noted, the certificate will contain very little information. The Commission itself acknowledged that this ground of refusal will apply to exceptional cases only, for instance to an order requesting the production of content data pertaining to undefined group of people in a geographical area or with no link to concrete criminal proceedings.[163] Finally, it should be noted that service providers are not obliged to assess this ground for refusal before executing EPOs.[164] By contrast, service providers must execute EPOs and EPsOs[165] and may be sanctioned for failing to do so (see *infra*). At

[161] According to art. 8(3) of the proposed Regulation, the certificate for production orders will contain the information listed in art. 5(3)(a) to (h) of the proposed Regulation which does not include the grounds for the necessity and proportionality of the measure. For preservation orders, under art. 8(4) of the prosed Regulation, the certificate will contain the information listed in art. 6(3)(a) to (f) which does not include the grounds for the necessity and proportionality of the measure.

[162] EDRi, 'Position Paper on the European Commission's Proposal for a Regulation on European Production and Preservations Orders for Electronic Evidence in Criminal Matters' cit. 20.

[163] Explanatory Memorandum cit. 21.

[164] See art. 9(5)(2) of the proposed Regulation.

[165] Art. 9(1) of the proposed Regulation states that service providers "shall ensure that the requested data is transmitted". Art. 10(1) states that the service provider "shall, without undue delay, preserve the data requested".

the enforcement stage, service providers "may oppose" the enforcement of EPOs[166] and EPsOs[167] when "based on the sole information contained in the [order], it is apparent that it manifestly violated the Charter or that it is manifestly abusive".[168] Then, it will be for the enforcing authority to decide whether or not to enforce the order[169] which means that even if the service provider's legal representative had opposed the order on fundamental rights' ground, he may nevertheless be obliged to execute it.

The Council did not address the aforementioned issues, instead it deleted the human rights clause from grounds upon which service providers are permitted to refuse to execute production orders [170] and from the list of grounds upon which service providers may oppose the enforcement of an order.[171] As a consequence, in the General Approach the responsibility to protect fundamental rights lies solely with the issuing State. This goes even further than the Commission's approach and the General Approach gave rise to harsher criticisms than the Commission's Proposal.[172] The European Parliament intends to reverse the paradigm shift and return to a traditional mutual recognition approach. The Report adopted by the European Parliament prevents service providers from becoming legal assessors of fundamental rights (see *infra*). Prior to the Report being released, the LIBE Committee's *Rapporteur* had stated that the wording of the human rights clause was very vague and suggested to replace it with the definition from art. 11(1)(f) of the EIO Directive: "there are substantial grounds to believe that the execution of the investigative measure indicated [in the EIO] would be incompatible with the executing State's obligations in accordance with art. 6 TEU and the Charter". She considers that a fundamental rights clause has to be sufficiently broad referring to all rights and to art. 6 TEU which covers the three layers of fundamental rights protection, namely: the ECHR, the EU Charter and common constitutional tradition.[173]

[166] *Ibid*. art.14(4).

[167] *Ibid*. art. 14(5).

[168] *Ibid*. art. 14(4) (f) and (5)(e).

[169] *Ibid*. art. 14(6).

[170] See art. 9(5) of the General Approach cit.

[171] *Ibid*. art. 14(4) and (5).

[172] See C Berthélémy, 'EU Council's General Approach on "e-Evidence": From Bad to Worse' (19 December 2018) edri.org; at least seven EU States, including Germany, opposed the Council's draft. The Netherlands, for instance, denounced the Council's text for being adopted "too fast" and stated that it "opened the way for abuse by EU countries that lack sufficient guarantees over the rule of law and fundamental rights". See T Christakis, 'Lost in Notification? Protective Logic as Compared to Efficiency in the European Parliament's e-Evidence Draft Report' cit.

[173] EP (LIBE Committee), 6th Working Document (B) cit. 3. The *Rapporteur* noted that "taking over the same wording as the EIO seems to be even more important in order to overcome the current patchwork of clauses from different EU mutual recognition legal instruments and CJEU case-law. Even though it has become clear over time that a clear fundamental rights clause is essential for guaranteeing fundamental rights obligations, the practice has rather been to introduce different clauses for each mutual recognition instrument, with a clear intention by some to limit it or render it inapplicable".

Secondly, considerations of a more practical nature must be taken into account if EU institutions were to consider giving a role to service providers. First, it can be noted that the time-limit for compliance with EPOs are pretty strict.[174] The mandatory deadline is ten days maximum upon receipt of the certificate and this deadline is reduced to six hours in case of emergency.[175] It has been claimed that these time-limits are too short to allow for a proper assessment of whether there are any grounds not to comply with the order and take appropriate decision.[176] Some consider that it will certainly not allow for an in-depth assessment of human rights issues.[177] EuroISPA, the world's largest association of internet service providers, warned that the timeframes are not feasible for small and medium enterprises (SMEs), especially the six hours deadline. According to the association, this deadline is not practicable for a vast majority of its members.[178] In addition to time constraints, undertaking a human rights assessment requires financial and personal resources. Unfortunately, the proposed Regulation does not harmonise the reimbursement of costs. Art. 12 of the proposed Regulation specifies that service providers may claim reimbursement of their costs by the issuing State if it is provided by the national law of that State. Therefore, depending on the national law of the issuing Member State, service providers may or may not be reimbursed for the costs of their cooperation. It could be argued that big companies such as Facebook and Microsoft, contrary to SMEs, do have the means and resources to comply with strict deadlines and perform human rights assessment. Nevertheless, big companies receive a staggering number of requests.[179] The question of who should bear the cost of cooperation needs to be addressed. While the Council General Approach follows the Commission's approach,[180] the

[174] For EPsOs, art. 10(1) of the proposed Regulation provides that upon receipt of the certificate, "the addressee shall, without undue delay, preserve the data requested".

[175] See art. 9(1) and (2) of the proposed Regulation. An emergency case is defined as a situation where there is an imminent threat to life or physical integrity of a person or to a critical infrastructure. See Explanatory Memorandum cit. 19.

[176] Opinion 23/2018 cit. 6; Opinion 7/2019 cit. para. 62; EDRi, 'Position Paper on the European Commission's Proposal for a Regulation on European Production and Preservations Orders for Electronic Evidence in Criminal Matters' cit. 5. The EDPS and EDRi recommended to make the six hours deadline for emergency cases a preferred time-limit rather than a mandatory one. See Opinion 7/2019' cit. para. 65; EDRi, 'Position Paper on the European Commission's Proposal for a Regulation on European Production and Preservations Orders for Electronic Evidence in Criminal Matters' cit. 5.

[177] M Böse, 'An Assessment of the Commission's Proposals on Electronic Evidence' cit. 41.

[178] EuroISPA, 'Position Paper on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters' (June 2018) www.euroispa.org 2.

[179] For an overview of the number of requests from law enforcement authorities received by Microsoft, for instance, see www.microsoft.com.

[180] See art. 12 of the General Approach cit.

European Parliament Report opens the possibility for service providers to obtain reimbursement of the costs exposed to cooperate with law enforcement authorities.[181]

Finally, unlike a public authority, service providers will be subject to an obligation to produce or preserve the requested data, and will be confronted with the risk to be subjected to enforcement measures and pecuniary sanctions in case of non-compliance.[182] Indeed, under art. 13 of the proposed Regulation, Member States are required to enact rules on pecuniary sanctions applicable to infringements of the obligations to execute EPOs and EPsOs.[183] The proposed Regulation does not include specific minimum rules, it refers, as for the reimbursement of costs, to national law and solely requires Member States to provide "effective, proportionate and dissuasive" sanctions. In the Council General Approach sanctions of up to 2 per cent of the total worldwide annual turnover of the service provider's preceding financial year can be imposed. It is not unreasonable to argue that such a sanction may deter service providers from objecting to EPOs and EPsOs.[184] However, service providers have obligations towards their customers under the GDPR. Service providers may legitimately ask what would be the consequences of not opposing the execution or the enforcement of an order that does actually violate the Charter. Can a service provider be held responsible for such violation? The proposed Regulation[185] does not offer much guarantee to service providers nor does the Council General Approach[186] – a statement is simply included in the Recitals – whereas the European Parliament Report provides that, "without prejudice to data protection obligations", service providers shall not be held liable in Member States for the consequences resulting from compliance with an EPOC or an EPsO.[187] The European Parliament also abandons the Council General Approach punitive sanction of up to 2 per cent of the total worldwide annual turnover of the service provider's preceding financial year case in case of non-

[181] Art. 12 of the European Parliament Report provides that "where so claimed by the service provider, the issuing State shall reimburse the justified costs borne by the service provider and related to the execution of the European Production order or the European Preservation Order".

[182] M Böse, 'An Assessment of the Commission's Proposals on Electronic Evidence' cit. 41.

[183] Pecuniary sanctions shall also be applicable to infringements of the obligations pursuant to art. 11 of the proposed Regulation which relates to the confidentiality of production and preservation orders.

[184] T Christakis, 'Lost in Notification? Protective Logic as Compared to Efficiency in the European Parliament's e-Evidence Draft Report' cit.; EDPS, 'Opinion 7/2019', cit., para. 66; EDRi, 'Position Paper on the European Commission's Proposal for a Regulation on European Production and Preservations Orders for Electronic Evidence in Criminal Matters' cit. 17.

[185] Recital 46 of the proposed Regulation: "Notwithstanding their data protection obligations, service providers should not be held liable in Member States for prejudice to their uses or third parties exclusively resulting from good faith compliance with an EPOC or an EPOC-PR".

[186] Recital 46 of the General Approach: "Service providers should not be held liable in Member States for prejudice to their uses or third parties exclusively resulting from good faith compliance with an EPOC or an EPOC-PR. The responsibility to ensure the legality of the Order, in particular its necessity and proportionality, should lie with the issuing authority".

[187] Art. 13(1a) of the European Parliament Report cit.

compliance with orders. Art. 13(1) of the Report refers to sanctions that "shall be effective, proportionate and dissuasive", as did the Commission in its proposed Regulation.

In terms of costs and responsibility, the European Parliament Report puts service providers a much more comfortable situation which is unmistakably linked to the limited role granted to these private actors in the Report. As briefly mentioned earlier, the European Parliament intends to reverse the paradigm shift and to prevent service providers from becoming legal assessors of fundamental rights.[188] The responsibility to protect fundamental rights would remain with the issuing State and the executing State. The change of terminology between the Commission's Proposal – enforcing State – and the Report – executing State – is, again, no coincidence. The Report provides that EPOs and EPsOs shall be addressed to the service provider and to the executing authority (in the State of the service provider) simultaneously.[189] By comparison, the Draft Report provided that, in addition, the EPOs shall be addressed simultaneously to the affected State (i.e. the state of residence of the data subject concerned by the EPO) "where it is clear that the person whose data is sought is residing neither in the issuing State nor the executing State".[190] This implied that EPOs would potentially have had three different addressees.[191] The notification system contained in the Report gives a prominent role to the executing State. This means that countries hosting several service providers, or the one of most important players such as Facebook, will find themselves assailed by EPOs and face a very heavy workload.[192]

For EPOs relating to subscriber data and IP addresses and for EPsOs, while the order is addressed directly and simultaneously to the executing authority, the Report provides that the information of the executing authority "shall not have a suspensive effect on the obligation of the service provider" to transmit or preserve the data.[193] In case of an EPO for subscriber data and IP addresses, the service provider must ensure that the data is

[188] European Parliament Draft Report cit. 146.

[189] Art. 7(1) of the European Parliament Report cit.

[190] Amendment 130 of the Draft Report cit.

[191] However, each addressee would have had different prerogatives. While the executing State could object EPOs on several grounds that include a human rights clause identical to the one contained in the EIO Directive (see Amendment 142 of the European Parliament Draft Report cit.), the affected State did not have such a capacity. The affected State could only inform the executing State if the former considers that one of the grounds for non-recognition or non-execution applies (see Amendment 146 of the European Parliament Draft Report). While this mechanism is certainly an improvement in terms of fundamental rights protection compared to the Commission's proposed Regulation and the Council General Approach one may legitimately question whether it would create negative repercussions on the efficiency of the instrument. As a matter of fact, the Draft Report has provoked a strong reaction from the Commission. The institution claimed that the amendments suggested by the LIBE Committee's *Rapporteur* would have a major impact on the efficiency of the e-Evidence Proposal. See T Christakis, 'Lost in Notification? Protective Logic as Compared to Efficiency in the European Parliament's e-Evidence Draft Report' cit.

[192] Théodore Christakis notes that it is not surprising that Ireland was in favor of notifying the Member State where the person whose data are sought is residing. See T Christakis, 'E-Evidence in a Nutshell: Developments in 2018, Relations with the CLOUD Act and the Bumpy Road Ahead' cit.

[193] See arts 8a(1) and 10(1a) of the European Parliament Report cit.

transmitted directly to the competent authority in the issuing state, as soon as possible and at the latest 10 days upon receipt of the EPO[194] or within 16 hours in case of emergency.[195] The executing authority has 10 days to invoke a ground for non-recognition or non-execution.[196] If the executing authority invokes such a ground, the Report provides that if the data have not yet been transmitted to the issuing authority, the service provider shall not transmit the data.[197] However, the Report does not impose the obligation for the issuing authority to erase the data in case it would have been transmitted before the executing authority invoked a ground for non-recognition or non-execution. Regarding EPOs for traffic data and content data, under art. 9(1a) of the Report, the executing authority must decide whether or not to refuse the execution of the EPO based on the grounds for non-execution or non-recognition listed in art. 10a which includes a human rights clause.[198] The deadline for the executing authority to refuse to execute the EPO is identical to the deadline to invoke grounds for non-execution or non-recognition in relation to EPOs for subscriber data and IP addresses.[199] The service provider may transmit the data directly to the issuing authority where the executing authority has not invoked any grounds for non-execution or non-recognition within 10 days upon receipt of the EPPO.[200] Furthermore, the Report also conditions the transmission of traffic data and content data to the explicit written approval of the executing authority if the issuing State is subject to a procedure under art. 7(1) or (2) of the Treaty on the European Union. In other words, service providers are not allowed to transmit traffic data and content data to Member States being subject to infringement proceedings for violations of EU law without the approval of the executing State.

Regarding the role of service providers, the Report allows these private actors to flag issues with EPOs and EPsOs and uses a language similar to the Commission's Proposal. Indeed, the Report specifies that service providers may inform the executing authority that an EPO or EPsOs is manifestly abusive or exceeds the purpose of the order.[201]

To conclude, it makes no doubt that putting service providers in the position of protecting European citizens' fundamental rights raises questions. As discussed above, one may ask if these private actors are sufficiently equipped and knowledgeable to assess the impact of an order on the fundamental rights of the person concerned. We should also ask whether these actors are willing to play a part. Telecommunications operators, for

[194] *Ibid*. art. 8a(2). The service provider also has the obligation to simultaneously send a copy of the data transferred for information to the executing authority.

[195] Art. 8a(3) of the European Parliament Report cit.

[196] *Ibid*. art. 8a(4). The executing authority must immediately inform the service provider and the issuing authority of its decision.

[197] *Ibid*.

[198] *Ibid*. see art. 10a(1)(c).

[199] *Ibid*. art. 9(1a).

[200] *Ibid*. art. 9(2b).

[201] *Ibid* arts 8a(7), 9(5)(2) and 10(6).

instance, have clearly shown reluctance and stated they did not want to adjudicate on citizen's fundamental rights and they were not in position to do so.[202] Microsoft, however, saw the Commission's Proposal as a "positive step forward".[203] BSA | The Software Alliance, the leading advocate for the global software industry, welcomed the Commission's Proposal while expressing concerns over the timeframes for compliance and emphasized that adequate time is needed for service providers to evaluate all data requests.[204] It is now up to the EU institutions to decide whether it is feasible and, more importantly, acceptable for private actors to play a role in the protection of fundamental rights and, if so, to what extent. In this regard, it may be worth noting that even those who are among the most critical towards the Commission's Proposal, such as EDRi, have acknowledged that service provider might play a role in assessing the intrusiveness of law enforcement demands as they are best placed to know about the nature and amount of data requested and the technicalities related to the production and transfer of data.[205] Service providers can flag issues that may not be identified or dealt with by the States concerned.[206] It is also important to recall that service providers have obligations towards their customers in terms of data protection (see *supra*). Whatever the European institutions will decide, the Commission's Proposal has left room for improvement. The analysis on the limited role of service providers provided above, clearly indicates that the Commission did not intend for service providers to fill the shoes of an executing State.[207] This creates a situation where the issuing State would be the sole guardian of fundamental rights and has been considered unacceptable for some of the stakeholders involved, especially the European Parliament.

[202] EP (LIBE Committee), 3rd Working Document (A) cit. 4; EuroIspa strongly advocates against service providers becoming actors responsible for checking orders against the local or the Issuing Member State's law as well as to signal non-compliant or abusive orders. See EuroISPA, 'Position Paper on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters'cit. 1; for the Deutsche Telekom see A Petri, 'No Law Enforcement by Private Corporations' (10 May 2018) www.telekom.com.

[203] J Frank and L Cossette, 'The e-Evidence Proposal – A Positive Step Forward' (18 April 2018) Microsoft EU Policy Blog blogs.microsoft.com.

[204] BSA | The Software Alliance, 'BSA Welcomes Draft EU e-Evidence Legislation. Advocates for continued dialogue' (16 April 2018) www.bsa.org.

[205] EDRi, 'Position Paper on the European Commission's Proposal for a Regulation on European Production and Preservations Orders for Electronic Evidence in Criminal Matters' cit. 25.

[206] See T Christakis, '"Big Divergence of Opinion" on e-Evidence in the EU Council: A Proposal in Order to Disentangle the Notification Knot' (22 October 2018) Cross-Border Data Forum www.crossborderdataforum.org.

[207] M Stefan and G Gonzalez Fuster consider that "the very rationale underlying the different provisions on the role of service providers does not, as a matter of fact, appear to be concerned with effectively replacing judicial authorities in terms of rule of law requirements, but rather with facilitating their intervention, and mitigating some possible conflicts". See M Stefan and G González Fuster, 'Cross-Border Access to Electronic Data Through Judicial Cooperation in Criminal Matters – State of the Art and Latest Developments in the EU and the US' cit. 40.

V. Conclusions

The e-Evidence Proposal has led to an institutional confrontation between the Commission and the Council, on the one hand, and the European Parliament, on the other hand.[208] While the former plead for an instrument based on an efficiency logic, the latter is a strong advocate of fundamental rights – and their positions seem hardly reconcilable. Numbers speak louder than words. The Draft Report presented by the LIBE Committee's *Rapporteur* in October 2019 contained 267 amendments to the Commission's proposed Regulation and further amendments were brought forward by different political groups at the end of last year, raising the number of amendments to 841 in total.[209] Even though the European Parliament has, in some respects, softened its approach, the Report abandons some of mechanisms and basic principles contained in the Commission's Proposal, including the paradigm of direct cooperation with service providers and may hinder the efficiency of the instrument. The challenge ahead for EU institutions will be to create an instrument that can reconcile both approaches and will strike a right balance between efficiency and fundamental rights' protection. Indeed, on the one hand, a burdensome legal instrument will bring the risk that law enforcement authorities will try to circumvent. On the other hand, an instrument placing efficiency and law enforcement authorities' interest above fundamental rights will weaken the level of protection granted to the fundamental rights to respect for private life and to protection of personal data and may fail to meet the high standards set by the Court of Justice.

One can regret that, so far, the EU institutions have missed the opportunity to adopt a position on some important questions such as the instrument – the GDPR or the LED – that must apply when public authorities access data stored by private actors. Another question that, in our opinion, is crucial and must be addressed concerns service providers. The EU institutions must decide whether service providers may play a part in the protection of fundamental rights and, if so, how and to what extent. The European Parliament's *Rapporteur* is sceptical and so are other actors, including various service providers. Nevertheless, even those who were among the most critical ones towards the role assigned to service providers in the Commission's Proposal did acknowledge that service providers might play a useful role in some circumstances. Only the results of the trilogues will tell what role, if any, service providers will be given in the EU e-evidence framework.

[208] For an overview of the basic features of the European Parliament Draft Report see T Christakis, 'E-Evidence in the EU Parliament: Basic Features of Birgit Sippel's Draft Report' cit. For an opinion on whether the European Parliament Draft Report strikes a right balance between necessary protection and efficiency see T Christakis, 'Lost in Notification? Protective Logic as Compared to Efficiency in the European Parliament's e-Evidence Draft Report' cit.

[209] See European Parliament (LIBE Committee) Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters, Amendments 268-582 (AM\1193813) and Amendments 583-841 (AM\1194325).