Faculty of Law,
Economics
and Finance

Law Working Paper Series
Paper number 2018-010

Transborder Access to e-Evidence by Law Enforcement Agencies

A first comparative view on the Commission's Proposal for a Regulation on a European Preservation/Production Order and accompanying Directive

Mark D. Cole, University of Luxembourg
mark.cole@uni.lu

Teresa Quintel, University of Luxembourg, Uppsala University
teresa.quintel@uni.lu

05/11/2018

UNIVERSITÉ DU LUXEMBOURG

Transborder Access to e-Evidence by Law Enforcement Agencies

A first comparative view on the Commission's Proposal for a Regulation on a European Preservation/Production Order and accompanying Directive

Mark D. Cole and Teresa Quintel*

Introduction

As communication nowadays commonly takes place via electronic means and online, the use of electronic evidence (e-evidence) is becoming a crucial element in criminal investigations. Due to the borderless nature of the internet, many criminal investigations that take place in the 'offline world' include a cross-border dimension. They therefore commonly require access to electronic data and evidence that is stored outside the territorial jurisdiction of the investigating authority.

Since these data are typically held by private companies that are often located in a different country than the investigator, law enforcement authorities (LEAs) are either dependent on the willingness of these service providers to cooperate on a voluntary basis in order to have the data available for investigations, or resort to existing legal procedures. The relevant procedures under the current framework to access data stored outside the European Union (EU) is based on so-called Mutual Legal Assistance Treaties (MLATs), whereas judicial cooperation within the EU is, *inter alia,* governed by the Directive on the European Investigation Order (EIO) in the form of the national transposition acts.[1] The latter aims to make cross-border investigations across the EU faster and more efficient by using several investigative measures with a view to gathering evidence on the basis of mutual recognition. MLATs on the other hand provide for domestic judicial review in both the requesting and the receiving state. This is one of the reasons why the current MLAT procedure is said to imply practical challenges, which have to do with a bemoaned slowness as different judicial authorities have to be involved, the alleged lack of efficiency and the legal uncertainty within the prevailing MLAT regime.

Since electronic (=e-) evidence is, due to its volatile nature, prone to modification and deletion, timely acquisition of stored data is vital for LEAs. Therefore, informal cooperation between LEAs and private companies is a common method to obtain electronic evidence, thereby bypassing the Mutual Legal Assistance (MLA) mechanisms. Thus, whereas under MLATs a request for access to data would be sent to a judicial authority in the receiving state, direct cooperation often entails the issuing of a domestic investigative measure by the LEA directly to the (foreign) service provider. Such informal cooperation between LEAs and foreign service

* *Mark D. Cole* is Professor for Media and Telecommunication Law at the Faculty of Law, Economics and Finance of the University of Luxembourg and Director for Academic Affairs at the Institute of European Media Law (EMR) in Saarbrücken. *Teresa Quintel*, LL.M. is an FNR-funded Ph.D. student at the University of Luxembourg under supervision of Prof. Cole.

[1] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order. This relatively recent EU instrument replaced the necessity to rely on the previous bi- or multilateral agreements as they apply still with non-EU-States.

.

providers has progressively become one important channel to obtain non-content data.[2] This results in legal disputes about jurisdiction matters where the informal approach turns into a formal request. The tendency of state authorities to more proactively assert jurisdiction beyond their national borders in cyberspace, thereby bypassing the more time-consuming MLA procedures, implies that particularly service providers are increasingly confronted with conflict of laws concerns when they have to decide whether or not to comply with these requests.[3] From the company perspective the orientation towards the legal framework of the country with traditional jurisdiction – typically the seat state – and especially data protection concerns under that legal regime lead to an understandable hesitation to comply with such requests on an informal level. Direct cooperation between law enforcement and private companies, which is commonly carried out on an unilateral basis, has led to a fragmented framework, *inter alia,* due to differences in the types of data requested, divergent procedures for submitting requests, unreliable outcomes and unpredictable response times.[4]

Against this background, the European Commission (Commission), on 17 April 2018, proposed new rules on access to e-evidence and information, to secure and obtain e-evidence more quickly and effectively and to ensure that all providers that offer services in the Union are subject to the same obligations.[5] The proposal includes a Regulation[6] and a Directive[7] that aim to develop a common framework for cooperation with service providers for the purposes of obtaining specific categories of data and to improve legal certainty and clarity.

The proposed legal instruments must comply with the EU data protection *acquis,* consisting of Regulation (EU) 2016/679[8] (GDPR), which applies to general processing of personal data, and Directive (EU) 2016/680[9] (LED) that specifically covers processing in the law enforcement context. Thus, processing of personal data carried out by service providers will fall within the scope of the GDPR, whereas processing by law enforcement authorities for the purposes of the prevention, investigation, detection and prosecution of crime will be governed by the rules of

[2] Gavin Robinson, 'Data Protection and the European Production Order for Electronic Evidence in Criminal Matters' (Draft), May 2018; Vanessa Franssen, 'The European Commission's E-Evidence Proposal:Towards an EU-wide obligation for Service Providers to cooperate with Law Enforcement?', European Law Blog, 12 October 2018; http://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/.

[3] Cesare Bartolini, Cristiana Santos, Carsten Ullrich, 'Property and the cloud', Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005, p. 23.

[4] European Commission, 'Non-Paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace' ('Commission non-paper 1'), available via Council of the European Union, doc. 15072/1/16 REV (7 December 2016), para 1.2.1. http://data.consilium.europa.eu/doc/document/st-15072-2016-init/en/pdf.

[5] European Commission "E-Evidence," Migration and Home Affairs, February 7, 2017, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

[6] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Strasbourg, 17.4.2018.

[7] Proposal 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, COM(2018) 226 final, Strasbourg, 17.4.2018.

[8] 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 [2016]OJ L 119, p. 1–88.

[9] 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, [2016] OJ L 119, p. 89–131.

the LED. The compliance of the new rules on access to e-evidence with the EU data protection *acquis* will be one of the relevant matters covered in this article.

Meanwhile, similar developments concerning the adoption of legislative acts or other instruments regarding law enforcement access to data stored by private companies take place elsewhere. Exemplary for the area of Europe (and also beyond) the developments within the Council of Europe (CoE) can be mentioned and, because of the high relevance as far as IT companies are concerned, on an international level especially the United States of America. These developments will, together with the Commission's proposals, be discussed below in order to put the proposals into a comparative perspective.

This contribution will address concerns regarding the role of private companies as 'extended arm' of LEAs and discuss the impact of the proposals with regard to EU data protection standards. This will include looking at previous developments on EU level concerning a Directive that required telecoms operators to retain certain types of metadata for a long period from all customers and which was later quashed by the Court of Justice of the European Union (CJEU). Potential issues with regard to data protection rights need to be considered against the background whether there is a justified interest of LEAs to rely on effective measures to access data and to analyze personal data for investigation purposes.

The article will briefly describe the current procedures for cross-border access to electronic evidence (section I.), illustrate the initiatives that are currently on the table at the level of the CoE (section II. 1)) as well as across the Atlantic in the U.S. (section II. 2)). Section III. will present the EU proposals on access to e-evidence and the specific data protection issues concerned by the proposal in section IV. The Conclusion will summarize the main findings and point to certain aspects that should be taken into account when similar measures on different levels are being adopted.

I. Background: Mutual Legal Assistance and Mutual Recognition

Traditionally, Mutual Legal Assistance refers to a mechanism that facilitates cooperation between states for the purposes of gathering and exchanging information. Such cooperation commonly serves to assist in the investigation or prosecution of criminal offences with a cross-border dimension. Under MLA procedures, competent state authorities may request form another competent (foreign) state authority legal assistance by submitting a judicial decision that may be verified by the receiving state, which will then decide whether or not to comply with the request.

In the EU, cooperation in criminal matters mainly developed with the introduction of the Schengen Area, but was progressively replaced by mutual recognition instruments.[10] The principle of mutual legal assistance and, in the EU the principle of mutual recognition goes hand in hand and with mutual trust between the Member States. Moreover, mutual recognition requires a minimum harmonization of national laws, meaning that a criminal offence in one

[10] European Commission, 'Mutual Legal Assistance and Extradition', accessed June 2, 2018, https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en.

Member States must also constitute a criminal offence in the other Member States. Likewise, for MLA, the approximation of national criminal procedural laws is prerequisite in order to prevent conflicts regarding minimum standards.

The first European treaty on mutual legal assistance was the CoE's European Convention on Mutual Assistance in Criminal Matters, which was concluded on 20 April 1959.[11] This Convention was supplemented with a Protocol of 17 March 1978[12] and a Protocol of 8 November 2001.[13] The Council of Europe is a separate international organisation from the European Union and has 47 Member States but also allows for some of its Conventions – which are opened for signature to states and sometimes international organisations – to be signed and ratified by non-Member States. This allows the reach of CoE instruments to go well beyond the geographical limits of Europe. On the other hand, it needs to be noted that the organisation works purely on the basis of public international law treaties, which do not enable it to implement by supranational force "law" directly on the states bound by the treaties. It is noteworthy that for the European Convention on Human Rights (ECHR) there is a specific court set up that allows individuals to take complaints against States based on a violation of ECHR provisions to the European Court of Human Rights (ECtHR) in Strasbourg. However, the jurisdiction of that Court is limited to the ECHR and does not cover any of the other CoE instruments such as the ones mentioned here.

For the European Union (respectively the previous European Community) the establishment of the internal market in 1992 and the abolishment of the national borders within the Schengen Area in 1995[14] marked the beginning of closer cooperation in criminal matters among the EU Member States. Against that background, the Maastricht Treaty led to the creation of the so-called 'Third Pillar', giving the EU limited competences to legislate in certain criminal matters.[15] This pillar in those days was still an intergovernmental activity that had to rely on full support by all Member States, but in the meanwhile, with the entry into force of the Treaty of Lisbon in 2009, has been integrated fully into the only remaining pillar of the EU as supranational field of action.

The EU Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[16], established by the Council Act of 29 May 2000 in accordance with Article 34 of the Treaty on European Union was the first MLA instrument on EU level. Supplementing the provisions of the CoE and its 1978 Additional Protocol[17], the MLA

[11] European Convention on Mutual Assistance in Criminal Matters, ETS No.030, Strasbourg, 20 April 1959.

[12] The additional Protocol entered into force in Belgium on 29 May 2002 and in Luxembourg on 31 December 2000 (http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=099&CM=8&DF=24/08/2014&CL=ENG).

[13] The second additional Protocol entered into force in Belgium on 1 July 2009 but has not yet been ratified by Luxembourg (http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=182&CM=8&DF=24/08/2014-&CL=ENG).

[14] European Commission, 'Schengen Area', https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen_en.

[15] Sanja Glaser / Andreas Motz / Frank Zimmermann, 'Mutual Recognition and its Implications for the Gathering of Evidence in Criminal Proceedings: A Critical Analysis of the Initiative for a European Investigation Order', THEMIS 2010/Barcelona.

[16] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *O.J.* C 197, 12 July 2000, 1 (hereinafter: EU MLA Convention). This Convention was supplemented with a Protocol on 16 October 2001: *O.J.* 326, 21 November 2001, 2.

[17] Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, ETS No.099, Strasbourg, 17.03.1978.

Convention's aim was to facilitate the application of those legal instruments, without affecting more favourable provisions in bilateral or multilateral agreements between Member States.[18] Unlike previous international MLA agreements, the EU MLA Convention contains explicit provisions on the interception of telecommunications.[19]

Council Framework Decision 2008/978/JHA[20] of 18 December 2008 established the European Evidence Warrant (EEW) for the purposes of obtaining objects, documents and data for use in proceedings in criminal matters in order to further enhance mutual assistance in the field of gathering evidence. It supplemented a Framework Decision from 2003 on the execution of orders freezing property and evidence in the European Union, which had been the first instrument that implemented the principle of mutual recognition in the field of obtaining evidence.[21]

As mentioned above, the principle of mutual recognition builds on mutual trust between the Member States, as judicial decisions from one Member State shall be recognized in another Member State. Thus, under those instruments, legality, necessity and proportionality of a request are being verified by the authorities in the requesting Member State and do not have to pass additional procedures of recognition in the receiving Member State.[22]

In 2009, the Lisbon Treaty codified the principle of mutual recognition under Articles 67 (3) and 82, the latter granting the European Parliament (EP) and the Council the power to adopt legislative acts to facilitate mutual recognition of judgments and judicial decisions under paragraph 2.

Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO)[23] is based on the principle of mutual recognition and aims to facilitate the gathering and transmission of evidence in criminal matters between the Member States. The EIO supplements the EEW by adding certain provisions and expanding its scope while maintaining some of the rules of the Framework Decision. Covering the entire process from the freezing of evidence to the transfer of existing evidence, the EIO's main objective is to reduce the level of fragmentation for the gathering of evidence and to establish a more coherent instrument that is applicable to additional types of evidence.[24] Moreover, it sets stricter deadlines to accept and answer requests, limits grounds for refusal of requests, and introduced

[18] Art. 1 EU MLA Convention. The EU MLA Convention also supplements and repeals certain provisions on mutual assistance in criminal matters of the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 (Art. 1 and 2 (2) EU MLA Convention).
[19] Art. 17 to 22 EU MLA Convention.
[20] Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters *O.J.* 350, 30 December 2008, 72 (hereinafter: Framework Decision on the EEW).
[21] Sanja Glaser / Andreas Motz / Frank Zimmermann, 'Mutual Recognition and its Implications for the Gathering of Evidence in Criminal Proceedings: A Critical Analysis of the Initiative for a European Investigation Order', THEMIS 2010/Barcelona, p. 7.
[22] On the mutual recognition principle cf., among others, Ormazábal Sánchez, Espacio penal europeo y mutuo reconocimiento, 2006; Jimeno Bulnes, European Law Journal 9 (2003), 614-630; Bujosa Vadell, Derecho penal supranacional y cooperación jurídica internacional, Cuadernos de Derecho Judicial XIII, 454; Gleß, ZStW 116 (2004), 353- 367; Peers, Common Law Market Review 41 (2004), 5.
[23] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *O.J.* 130, 1 May 2014, 1 (hereinafter: Directive on the EIO).
[24] Lorena Bachmaier Winter, 'European investigation order for obtaining evidence in the criminal proceedings. Study of the proposal for a European directive', in: Zeitschrift für Internationale Strafrechtsdogmatik, No. 9/2010, p. 581.

a standard format to submit requests to overcome language barriers.[25] The EIO marked a further step from the principle of MLA to mutual recognition in obtaining evidence taken by the European legislators.

II. Cross-border access to data on the international level

The idea of allowing access to data across borders has been discussed and developed not only within the European Union but also elsewhere on the international level. An early form of cooperation concerning "internet-related crime", then so-called cybercrime, was the still highly relevant "Budapest Convention" (or Cybercrime Convention) of the CoE: the Convention on Cybercrime of 23 November 2001 and its Additional Protocol concerning specific forms of crimes such as dissemination of incitement to hatred. Also there have been discussions on the level of the CoE to supplement the Convention with a Second Additional Protocol concerning cross-border access and refining a specific article of the Convention. This process started before the EPO proposal of the European Commission for the European Union and will most likely finish after the agreement on the final version of the EPO.

Below, the main elements of the Cybercrime Convention and further development in the CoE will be presented as well as an important international example for comparison – the U.S. approach for cross-border access to data is highly disputed there, too, as major IT companies storing data on European customers on EU territory have been requested to hand over such data to U.S. LEAs and a potentially ground-breaking case has been muted before the U.S. Supreme Court because of a recent related Act that was passed by Congress.

1. The Situation in Europe apart from the European Union: Council of Europe

a) The CoE Cybercrime Convention

The CoE's Budapest Convention on Cybercrime[26] has been open for signature since 2001 and entered into force in July 2004.[27] Until March 2018, 71 states, out of which 56 became parties to the Convention, signed it or were invited to accede.[28] With an exception of Ireland and Sweden, the Cybercrime Convention has been ratified by all of the EU Member States.[29]

Dealing with internet-enabled crimes, the Convention establishes international mechanisms for cooperation against cybercrime[30] and obliges its members to set up procedures to acquire electronic evidence within a mutual legal assistance framework. In that context, parties to the

[25] "European Commission Press Release, 'As of Today the 'European Investigation Order' Will Help Authorities to Fight Crime and Terrorism', accessed June 4, 2018, http://europa.eu/rapid/press-release_IP-17-1388_en.htm.
[26] Convention on Cybercrime, ETS No.185, Budapest, 23/11/2001.
[27] The Convention was so far ratified by 43 out of 47 Members of the Council of Europe (San Marino, Ireland, Russia and Sweden have not ratified it) and USA, Canada, Israel, Chile, Costa Rica, Dominican Republic, Japan, Mauritius, Panama, Senegal, Sri Lanka, Tonga and Australia. See: Paul de Hert, Cihan Parlar and Juraj Sajfert, 'The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law', in: computer law & security review (2018), p. 2.
[28] CoE: Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention, Version 19 March 2018, p. 1.
[29] CoE, Chart of signatures and ratifications of Treaty 185 Convention on Cybercrime, status as of 30/05/2018.
[30] In the 2013 Cybersecurity Strategy of the European Union, the Budapest Convention was recognized as the main multilateral framework for the fight against cybercrime - Joint Communication of the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final. COM(2018) 225 final, p. 4.

Convention are required to introduce production orders and preservation orders, the former in order to either obtain data from service providers in their territory or subscriber data from service providers offering services in their territory, the latter in cases where there are grounds to believe that data is particularly prone to modification or deletion.[31] Due to the challenges to enforce national production orders outside the territorial reach of members to the Convention, additional measures regarding cross-border access to e-evidence are currently being negotiated.[32]

Article 18 of the Cybercrime Convention stipulates that parties to the Convention shall adopt measures to empower their competent authorities to issue production orders either against a person (Article 18.1.a.) or against a service provider offering its services in the territory of the party (Article 18.1.b.). With regard to a person in the territory of the party, the Explanatory Report states that a person would have to provide specified computer data stored in a computer system, or data storage medium that is in that person's possession or control.[33] According to the Explanatory Report, Article 18.1.b. requires a service provider offering services in its territory to 'submit subscriber information in the service provider's possession or control'.[34]

Article 32 of the Convention addresses international cooperation, in particular mutual assistance regarding investigative powers. The Article deals with unilateral trans-border searches where data are publicly available (Article 32.a. on trans-border access to publicly available (open source) stored computer data) or were data are disclosed on a voluntary basis (Article 32.b. on trans-border access with consent).[35]

The relationship between Article 18 and Article 32 of the Cybercrime Convention is somewhat ambiguous, as Article 18 could be interpreted as including access to data stored abroad, since it refers to information in the service provider's possession or control. Similarly, the wording 'offering services' in the party's territory could be understood as also covering data outside the territory of the state that is party to the Convention.[36]

b) The Planned Second Additional Protocol to the Cybercrime Convention

The so-called Cybercrime Convention Committee (T-CY) assesses the quality of national implementation acts of the Cybercrime Convention and considers solutions to challenges of criminal justice and the rule of law in cyberspace.[37] From 2012 to 2017, two experts groups, the Working Group on transborder access to data and the Cloud Evidence Group[38], were tasked

[31] COM(2018) 225 final, p. 4.
[32] Cybercrime Convention Committee (T-CY) Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime, Discussion Guide for consultations with civil society, data protection authorities and industry, T-CY (2018)16, Strasbourg, 21 May 2018, p. 3.
[33] Cybercrime Convention Committee (T-CY) T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention), Adopted by the T-CY following the 16th Plenary by written procedure (28 February 2017), T-CY(2015)16, Strasbourg, 1 March 2017, p. 4.
[34] Ibid.
[35] Paul de Hert, Cihan Parlar and Juraj Sajfert, 'The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law', in: computer law & security review (2018), p. 3.
[36] Ibid, p. 7.
[37] CoE, 'Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention', Version 19 March 2018.
[38] See: https://www.coe.int/en/web/cybercrime/ceg.

to develop instruments to further regulate the trans-border access[39] to data, the use of trans-border investigative measures, and to explore solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions.

In September 2016, the T-CY Cloud Evidence Group in its Recommendations on criminal justice access to data in the cloud recommended starting negotiations regarding an additional Protocol to the Cybercrime Convention. The objective of that protocol would be to facilitate direct cooperation with service providers in other jurisdictions by extending the scope of Article 32 of the Cybercrime Convention in order to allow for more effective mutual legal assistance.[40] The provisions on more effective MLA would include the expedited disclosure of the identity and physical address of the subscriber of a specific IP address or user account[41], would be applicable in situations where Article 18 is not applicable or cannot be enforced[42], or where a service provider refuses to respond to domestic production orders from competent authorities[43].

Moreover, the possibility and scope of an international production order to be directly sent by the authorities of one party to the law enforcement authorities of another party[44], and the establishment of joint investigation teams between the parties to the Convention as means for investigating transnational cases of cybercrime should be considered.[45] According to the T-CY, the latter option should also be available to states that are not parties to the Convention.[46]

In order to avoid delays for responses to international requests, the anticipated Protocol to the Cybercrime Convention should also allow for requests to be sent in English[47] and for emergency procedures concerning requests related to risks of life and similar exigent circumstances[48]. Further, the national legislation implementing Article 18 of the Cybercrime Convention should make data received from service providers admissible as evidence in criminal proceedings[49], and trans-border access without consent but with lawfully obtained credentials, in good faith or in exigent or other circumstances[50] should become an option.

These considerations were discussed during the second meeting of the T-CY Protocol Drafting Group in February 2018, where the Group also welcomed the developments on EU level regarding electronic evidence and criminal justice in cyberspace. According to the Group, the drafting of the additional protocol should be closely coordinated with the relevant legal instruments by the European Union.[51]

[39] Transborder Group, see: https://www.coe.int/en/web/cybercrime/tb.
[40] Cybercrime Convention Committee (T-CY), Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY', Final report of the T-CY Cloud Evidence Group, T-CY (2016)5, 16 September 2016 Strasbourg, France, p. 49 at 106 and 107.
[41] Ibid., note 110.
[42] Ibid., note 111.
[43] Ibid., note 114.
[44] Ibid., note 115.
[45] Ibid., note 125.
[46] Ibid., note 126.
[47] Ibid., note 130.
[48] Ibid., note 134.
[49] Ibid., note 138.
[50] Ibid., note 144.
[51] Cybercrime Convention Committee (T-CY) Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime, Summary report of the 2nd Meeting of the T-CY Protocol Drafting Group (Strasbourg 31 January – 2 February 2018), T-CY (2018)8, Strasbourg, 2 February 2018, p. 2.

2 The Situation in the United States of America

a) The Microsoft Corp. v. United States Case

In 2013, Microsoft, an U.S. incorporated and headquartered multinational technology company, received a warrant from the U.S. Government, requiring the disclosure of email content of a user's email account hosted by Microsoft. The warrant established probable cause on the assumption that the user conducted criminal drug activity via that email account. The warrant was issued under 18 U.S.C. 2703 of the Stored Communications Act (SCA)[52], requiring Microsoft to produce 'information associated with' the email account that was 'stored at premises owned, maintained, controlled, or operated by Microsoft Corporation'.[53]

While Microsoft disclosed the account identification records data stored on American servers, it did not provide email content data that was stored at a Microsoft data center in Dublin, Ireland. Microsoft argued that the Government's warrant did not cover information stored outside the United States[54] and decided to 'quash the warrant to the extent that it direct[ed] the production of information stored abroad'.[55] The argument brought by Microsoft was that the information sought by the U.S. Government was based on the SCA, according to which the issued warrant would have to use 'the procedures described in the Federal Rules of Criminal Procedure'.[56] According to Rule 41 of the SCA '[f]ederal courts are without authority to issue warrants for the search and seizure of property outside the territorial limits of the United States'.[57]

In May 2014, a federal magistrate judge rejected Microsoft's non-compliance to provide the data and ordered Microsoft to produce the requested emails, holding that an SCA warrant is similar to a subpoena and, therefore, not bound by territoriality. As Microsoft had control over the material outside of the U.S., the court argued that the company must nevertheless comply with the SCA warrant.[58]

The judgment was reviewed by the District Court of the Southern District of New York, which upheld the magistrate judge's ruling. On appeal, the Second Circuit, however, decided to revoke the warrant 'insofar as it demands user content stored outside of the United States'.[59]

Following the Second Circuit's judgment, U.S. Department of Justice filed for review of the *Microsoft* case, submitting a Writ of Certiorari to the U.S. Supreme Court after a rehearing *en banc* had not been granted. The Government held that disclosure of the data would occur in the

[52] Stored Communications Act, codified at 18 U.S.C. §§ 2701–2712.
[53] 'United States v Microsoft Corp Gets a Supreme Court Hearing,' Constitutional Law Reporter, October 26, 2017, https://constitutionallawreporter.com/2017/10/26/united-states-v-microsoft-2017-2/.
[54] 'The US v. Microsoft Supreme Court Case Has Big Implications for Data | WIRED,' accessed June 5, 2018, https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/.
[55] In re Warrant, 15 F. Supp. 3d at 468.
[56] Id. at 470 (quoting 18 U.S.C. § 2703(a) (2012)); see also id. (outlining Microsoft's argument).
[57] Id. Rule 41 vests no authority in magistrate judges to issue warrants for foreign searches. See, e.g., In re Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 171 (2d Cir. 2008) (expressing skepticism that judges can issue warrants for overseas searches). Foreign searches are instead subject to a reasonableness test that, in the Second Circuit, balances the intrusion on the individual's privacy against the government interest in the search. See id. at 172. In: "In Re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.," accessed June 5, 2018, https://harvardlawreview.org/2015/01/in-re-warrant-to-search-a-certain-email-account-controlled-maintained-by-microsoft-corp/.
[58] Electronic Privacy Information Center, "EPIC - United States v. Microsoft," accessed June 5, 2018, https://www.epic.org/amicus/ecpa/microsoft/.
[59] Center.

United States and therefore, constitute a permissible domestic application of the SCA.[60] On 16 October 2017, the Supreme Court granted the Government's petition.

The international interest in the *Microsoft* case was observable by the number of *amicus briefs* that were filed with the Supreme Court in support of Microsoft. The signatories included European lawmakers, Members of Congress, leading technology companies, media organizations, legal scholars, computer scientists, trade associations and advocacy groups.[61] In addition, several Governments, the European Commission, the U.N. Special Rapporteur on the Right to Privacy, officials from law enforcement, intelligence and national security bodies, as well as E-discovery practitioners submitted further amicus briefs.

While the *Microsoft* case was still pending, the California Northern District court decided a similar case[62], in which Google was asked to provide user data stored on servers outside the U.S., again under an SCA warrant, but came to a different conclusion. The court adopted the holdings of the dissenting judges in the *Microsoft* case, arguing that the warrant would presume domestic application of the SCA. According to the court, Google had to comply with the warrant, regardless of where the data sought were stored, since the warrant was addressed to individuals at Google's U.S. Headquarters who were responsible for the data.[63]

Meanwhile, and before the *Microsoft* case was heard, On March 23, 2018, the U.S. Congress passed and the President signed the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which amended the SCA.[64] According to the U.S. Government, the CLOUD Act resolved the question presented in the *Microsoft* case by specifying that a service provider responding to an SCA order must produce information within its 'possession, custody, or control, regardless of whether such information is located within or outside of the United States'.[65] Under the CLOUD Act, the U.S. Government obtained a new warrant, and was now able to argue that Microsoft's sole objection, that the prior warrant was impermissibly extraterritorial, no longer applied.[66] With the entry into force of the U.S. CLOUD Act, the *Microsoft* case was mooted.[67]

b) The U.S. CLOUD Act

The U.S. CLOUD Act was signed on 23rd March 2018, essentially creating an alternative mechanism to obtain data outside the scope of MLATs. The CLOUD Act allows U.S. law enforcement authorities to require service providers to preserve or disclose communications data of their users that is stored outside U.S. territory.

Under Section 2523 of the CLOUD Act, the United States may enter into executive agreements[68] with qualifying foreign governments in order to directly access data held by U.S.

[60] "US v. Microsoft Litigation Provides the Supreme Court with a Rare Opportunity to Further Clarify and Define the Role of Comity in International Discovery Disputes," JD Supra, accessed June 8, 2018, https://www.jdsupra.com/legalnews/us-v-microsoft-litigation-provides-the-81750/.

[61] For a complete list of signatories, see: https://blogs.microsoft.com/datalaw/wp content/uploads/sites/149/2018/01/Complete-List-of-Amici-Signatories_FINAL-4.pdf.

[62] In re Search Warrant No. 16-960-M-01 to Google.

[63] On this cf. also Cesare Bartolini, Cristiana Santos, Carsten Ullrich, 'Property and the cloud', Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005, p. 23.

[64] As part of the Consolidated Appropriations Act, 2018, H.R. 1625, Div. V, 115th Cong., 2d Sess. (2018).

[65] Motion to vacate the judgment of the Court of Appeals and remand the case with Directions to dismiss as moot. On writ of certiorari to the United States of Appeals for the Second Circuit Motion. No. 17-2, March 2018, p. 2.

[66] Ibid.

[67] 'United States v. Microsoft Corporation,' Oyez, accessed June 5, 2018, https://www.oyez.org/cases/2017/17-2.

[68] To qualify for an agreement the US Attorney General must determine that a candidate country's domestic law affords robust substantive and procedural protections for privacy and civil liberties, based on open criteria, including respect for the rule of law and principles of non-discrimination; respect for international universal human rights (eg. protection from arbitrary and

technology companies in these contracting countries.[69] The foreign governments would be able to conclude such agreements by way of certification issued by the U.S. Attorney General, after a certain assessment of their fundamental rights standards.[70]

It is thereby mainly private companies that are involved in approving requests. Thus, a request would be directly submitted to the provider (Facebook, Microsoft, Google, etc.), which might handle those requests differently, depending on size and resources of the provider. This process could eliminate many safeguards that were established under the MLATs procedures, such as the approval of the request or the review of evidence.

Under the CLOUD Act, a provider of electronic communication services may file a motion to modify or quash a request where the provider believes that the customer or subscriber is not a U.S. person or does not reside in the U.S. and, where the provider is of the opinion that the required disclosure would create a material risk that the provider would violate the laws of a foreign government.[71]

This means that U.S. LEAs could request access to 'the contents of a wire or electronic communication and any record or other information' without having to comply with EU data protection standards, where the U.S. entered into an executive agreement with the EU, if there is no material risk of violation.

The review mechanisms of certified countries under the CLOUD Act are questionable: Where a country entered into an agreement with the U.S., the withdrawal of the certification would be nearly impossible and review of the standards in the certified country would only take place on a 5-year basis. This could become problematic with regard to countries in which the political situation is unstable or that have low human rights standards in place.

III. The Proposal for a EU Regulation European Preservation / Production orders

As has been shown above, there is a general trend towards extending jurisdiction extraterritorially when it comes to accessing electronic evidence. The question of preserving data and granting access to it for the purposes of the prevention, investigation, detection or prosecution of crime has been addressed on various occasions during the past years in the EU.

unlawful interference with privacy; fair trial rights; freedoms of expression, association and peaceful assembly; prohibitions on arbitrary arrest and detention; and prohibitions against torture and cruel, inhuman, or degrading treatment or punishment); clear legal mandates and procedures governing those entities of the foreign government that are authorised to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective oversight of those activities; sufficient mechanisms to provide accountability and appropriate transparency regarding the government's collection and use of electronic data; and a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet. See: US Department of Justice, Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism, July 15, 2016, ('DoJ Bill'), p. 2.

[69] 'CLOUD Act: Civil Society Urges US Congress to Consider Global Implications,' *EDRi* (blog), March 19, 2018, https://edri.org/cloud-act-letter-uscongress-global-implications/.

[70] Katitza Rodriguez, 'The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom', Electronic Frontier Foundation, April 9, 2018, https://www.eff.org/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom.

[71] §2713 (2)(A), Motions to quash or modify.

1. From Data Retention to other EU Instruments concerning e-Evidence

For instance, the EU Data Retention Directive[72] required telecommunications providers to retain certain data of their users from 6 months up to 24 months in order to grant law enforcement access for crime prevention and investigation purposes. Eight years after its adoption in 2006, the Directive was quashed in the *Digital Rights Ireland*[73] judgment by the CJEU, which held that the indiscriminate retention of personal data was disproportionate and in violation with Articles 7, 8 and 52(1) of the EU Charter. That argument was later upheld in the *Tele2/Watson*[74] judgment, where the Court declared that only targeted data retention measures would be permissible and law enforcement access to retained data could solely be granted for the purpose of fighting *serious* crime and would have to follow prior judicial authorization.[75]

Yet, the growing importance of obtaining electronic evidence for law enforcement purposes has, despite the CJEU's strict approach in the above judgments, been addressed by various initiatives, *inter alia,* the Commission's 2018 Work Programme[76]. That program suggests to finalize guidance for Member States on new possibilities for data retention after *Digital Rights Ireland* and *Tele / Watson* and to introduce measures to facilitate cross border access by law enforcement authorities to electronic evidence.[77]

As previously mentioned, within the EU, the use of MLA mechanisms that traditionally govern transnational cooperation, gradually shifted towards mutual recognition of judicial decisions, a procedure, which has most recently been codified in the Directive on the European Investigation Order. An EIO is a judicial decision, which has been issued or validated by one Member State to have one or several specific investigative measure(s) carried out in another Member State to obtain (electronic) evidence.[78] The EIO entered into force on 22 May 2017[79], but was already at that time transcended by new motions on how to improve the means for law enforcement to obtain access to e-evidence.

---

[72] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58, OJ, L 105/54, 13.4.2006.

[73] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* (C-293/12) and *Seitlinger* (C-594/12), ECLI:EU:C:2014:238, 8 April 2014. EDPL

[74] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige* AB (C-203/15) and *Watson* (C-698/15), ECLI:EU:C:2016:970, 21 December 2016. EDPL Cole/Quintel, '"Is there anybody out there?" –Retention of Communications Data: Analysis of the status quo in light of the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) Carolina Academic Press Global Papers Series (forthcoming 2019).

[75] On the ground-breaking judgment of the CJEU declaring the Data Retention Directive void cf. Franziska Boehm and Mark D. Cole, 'Data Retention after the Judgement of the Court of Justice of the European Union', study for the Greens/EFA Group in the European Parliament. Münster/Luxembourg, 30 June 2014, especially concerning measures such as PNR and border control, p. 73 et seq., 89 et seq., 101 et seq., available at http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm-Cole-data_retention-study-printlayout.pdf. On the further development Cole/Quintel, '"Is there anybody out there?" – Retention of Communications Data: Analysis of the status quo in light of the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) Carolina Academic Press Global Papers Series (forthcoming). For more recent relevant case law (Opinion 1/15) see also Cole/Quintel, 'Data Retention under the Proposal for an EU Entry/Exit System (EES): Analysis of the impact on and limitations for the EES by Opinion 1/15 on the EU/Canada PNR Agreement of the Court of Justice of the European Union legal Opinion for the Greens/EFA Group (European Parliament)

[76] Commission Work Programme 2018: An agenda for a more united, stronger and more democratic Europe, COM(2017) 650 final, Strasbourg, 24.10.2017.

[77] COM(2017) 650 final, Strasbourg, 24.10.2017, p. 8.

[78] Article 1(1) of the EIO Directive.

[79] See: European Commission Press Release, 'As of today the "European Investigation Order" will help authorities to fight crime and terrorism, Brussels, 22 May 2017, http://europa.eu/rapid/press-release_IP-17-1388_en.htm-

2. The development of a specific e-Evidence Proposal

In June 2016, three months after the terrorist attacks in Brussels, the Council adopted conclusions on improving criminal justice in cyberspace, requesting the Commission to deliver reports on the progress made with regard to improving cooperation with service providers, streamlining MLA and mutual recognition proceedings and reviewing the rules on enforcement of jurisdiction in cyberspace.[80]

With regard to enhancing the cooperation with service providers, the Council requested the Commission to 'develop a common framework for cooperation with service providers for the purpose of obtaining specific categories of data, in particular subscriber data, when allowed by third countries' legislation, or any other comparable solution that allows for a quick lawful disclosure of such data'.[81] To that end, the Commission was tasked to explore possibilities to use aligned tools to ensure swift procedures and to increase transparency and accountability of the process of securing and obtaining e-evidence.[82]

In a non-paper from December 2016, the Commission acknowledged that Member States and their judicial and law enforcement authorities had taken diverging approaches regarding investigatory measures granting access to e-evidence.[83] According to the Commission, the systematic use of MLA for all types of access requests for electronic evidence was increasingly viewed as problematic and time-consuming.[84] Consequently, and despite the efforts to achieve enhanced cooperation through mutual recognition, there had been a further shift from applying MLA mechanisms towards the use of informal channels between LEAs and (foreign) service providers to obtain electronic evidence.[85]

After an additional non-paper[86], during public consultations[87] and the issuing of an Inception impact Assessment, the Commission proposed, on 17 April 2018, new rules to facilitate access to e-evidence by police and judicial authorities. The proposal comprises a Regulation for the launch of European Production Orders (EPO) and European Preservation Orders (EPrO) and a Directive to oblige service providers offering services in the EU to designate a legal representative in the Union who would receive such orders from LEAs.[88] The proposal was tabled by the European Commission, having the exclusive competence for initiating legislative

[80] Council of the European Union, Council conclusions on improving criminal justice in cyberspace (9 June 2016) <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/council_conclusions_on_improving_criminal_justice_in_cyberspace_en.pdf> accessed on 11/06/2018.
[81] Ibid., p. 3.
[82] Ibid.
[83] Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 15072/1/16 REV 1, Brussels, 7 December 2016, p. 4.
[84] Ibid, p. 5.
[85] Katalin Ligeti and Gavin Robinson, 'Transnational Enforcement of Production Order for Electronic Evidence: Beyond Mutual Recognition?, in:Robert Kert and Andrea Lehner (eds.) *Vielfalt des Strafrechts im internationalen Kontext – Festschrift für Frank Höpfel zum 65. Geburtstag* (2018), p. 626.
[86] Non-Paper of the EU Commission services of June 2017, Improving Cross-border Access to Electronic Evidence: Findings from the Expert Process and Suggested Way Forward ('Commission non-paper 2').
[87] Public consultation on improving cross-border access to electronic evidence, see <https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminalmatters_
en> accessed 21 August 2017.
[88] European Commission, 'E-evidence-cross-border access to electronic evidence. Improving cross-border access to electronic evidence', https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

procedures in the European Union. It is now discussed both within the competent committees of the EP and within the Council of the European Union, which represents the 28 Member States. Typically, the legislative procedures continue with a common position developed by the Council and the EP signaling the changes they would like to see being made to the original proposal. This is then followed by a so-called trilogue, in which the Commission moderates between the positions of EP and Council to reach an agreement that is then formally confirmed by the plenary of the Parliament and the Council sitting in the relevant composition, before being published in the Official of the EU.

The following section will briefly describe the main features of the e-evidence proposals and address those provisions that could have an (negative) impact on EU data protection standards.

3. The Proposal for a Regulation and Directive

The e-evidence proposal lays down the rules under which competent judicial authorities in the European Union may order a service provider offering services in the Union to produce or preserve electronic evidence through European Production Orders (EPOs) or European Production Orders (EPrOs).[89] The Regulation would be applicable in all cases where the service provider is established or represented in a Member State other than the requesting Member State[90], thus, not to domestic procedures. The service providers covered by the Regulation are required to comply with production or preservation orders for electronic evidence, regardless of the location where the requested data are stored.[91]

The legal basis of the proposed Regulation is Article 82(1) TFEU, which relates to measures on judicial cooperation that may be adopted[92] to lay down rules and procedures for ensuring recognition of all forms of judgments and judicial decisions throughout the Union and to facilitate cooperation between judicial or equivalent authorities.[93] According to the Commission proposal, that Article also applies where a judicial authority in the issuing State addresses a legal person in another Member State, for instance when imposing obligations on it, regardless of whether a judicial authority in the other Member State is involved in the process.[94] However, when a production or preservation order is issued, a judicial authority needs to be involved as either issuing or validating authority.[95] Moreover, the judicial authority of the State executing the preservation or production order may intervene when necessary to enforce the decision.[96] Yet, whether the production orders envisaged under the EPO proposal, which would oblige service providers to directly transmit electronic evidence, constitute judicial cooperation within the scope of Article 82(1) TFEU is debatable.[97]

[89] Recital (15) of the e-evidence proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.
[90] Recital (15) of the e-evidence proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.
[91] Article 1(1) of the e-evidence proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.
[92] By the European Parliament and the Council, acting in accordance with the ordinary legislative procedure.
[93] In relation to proceedings in criminal matters and the enforcement of decisions. COM(2018) 225 final, Strasbourg, 17.4.2018, p. 5.
[94] Ibid.
[95] COM(2018) 225 final, Strasbourg, 17.4.2018, p. 16.
[96] Ibid.
[97] Katalin Ligeti and Gavin Robinson, 'Transnational Enforcement of Production Order for Electronic Evidence: Beyond Mutual Recognition?, in:Robert Kert and Andrea Lehner (eds.) *Vielfalt des Strafrechts im internationalen Kontext – Festschrift für Frank Höpfel zum 65. Geburtstag* (2018), p. 642.

The accompanying Directive obliges those service providers covered by the Regulation to designate a legal representative for the receipt of, compliance with and enforcement of decisions and orders issued for the purposes of gathering evidence in criminal proceedings.[98]

Pursuant to Article 8 of the proposed Regulation, a European Production Order is implemented where the requesting authority issues a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR). Under Article 7 of the proposal, both EPOCs and EPOC-PRs shall be addressed to the designated legal representative, who will be responsible for the reception and the timely and complete execution of an order.[99] In case of urgency, if the legal representative does not comply with an order, or where no legal representative has been appointed, orders may be addressed to any establishment of the service provider in the Union.[100]

The personal scope of the proposal applies to providers of electronic communications services[101] and information society services for which the storage of data is a defining component of the service provided to the user.[102] Moreover, Article 2(3)(c) includes internet domain name and IP numbering services[103] under the definition of service provider.

The scope of the proposed Regulation solely covers production and preservation orders that are issued during the pre-trial and trial phases of criminal proceedings, also covering legal persons, which may be held liable for criminal offences in the issuing State.[104]

IV. Data protection regime under the EPO

1. Relevant rules in the proposal

Processing of personal data under the EPO Regulation will have to take into account the relevant data protection *acquis,* consistent of the General Data Protection Regulation (GDPR) and the Data Protection Directive for Police and Criminal Justice Authorities (LED). The GDPR entered into application on 25 May 2018, while the LED had to be transposed by the Member States by 6 May 2018. The scope of the GDPR covers general processing activities by private and public bodies, while the Directive only applies when processing is carried out by competent authorities within the meaning of Article 3(7) LED for the purposes of the prevention, investigation, detection and prosecution of criminal offences.

Thus, while the processing of personal data by service providers falls within the scope of the GDPR, competent LEAs will have to apply the LED when processing personal data for law enforcement purposes. Being applicable for both cross-border and domestic processing[105], the

[98] European Commission Press Release, 'Security Union: Commission facilitates access to electronic evidence', Brussels, 17 April 2018, http://europa.eu/rapid/press-release_IP-18-3343_en.htm.
[99] COM(2018) 225 final, Strasbourg, 17.4.2018, p. 17 and 18.
[100] Ibid, Article 7(2), (3) and (4) of the e-evidence proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.
[101] As defined in Article 2(4) of the proposed Directive establishing the European Electronic Communications Code, see Article 2(3)(a) of the e-evidence proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.
[102] As defined in point (b) of Article 1(1) of Directive (EU) 2015/1535, see Article 2(3)(b) of the e-evidence proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.
[103] Such as IP address providers, domain name registries, domain name registrars and related privacy and proxy services.
[104] Article 2(3) of the e-evidence proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.
[105] The Directive's predecessor, Framework Decision 2008/977/JHA, was only applicable to cross-border processing of personal data in the law enforcement sector.

LED harmonizes the national laws in respect of the exchange of information between police and judicial authorities, whilst leaving certain discretion to the Member States.

However, due to the specific field in which the LED applies, processors are granted more flexibility, for instance with regard to data subjects' right to information. Thus, where notification would jeopardize ongoing investigations, processors may refrain from informing data subjects that their data are being processed.[106]

This logic is being reiterated under Article 11(1) of the EPO proposal, which stipulates that service providers shall '[…] refrain from informing the person whose data is being sought under an EPO in order not to obstruct the relevant criminal proceedings'. In accordance with Article 11(2), the issuing authority shall inform the data subject concerned about the production of his or her data[107], but may delay notification as long as this is necessary and proportionate to avoid obstructing the relevant criminal proceedings.

Article 11, the only Article concerned with data protection under the proposal, therefore is in line with Article 23 of the GDPR and Article 13 of the LED, albeit being less specific. Article 23 GDPR provides that controllers or processors may restrict data subject rights to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, whereas Article 13 LED refers to data subjects' right to information in the law enforcement context.

The task of imposing restrictions due to criminal proceedings is, therefore, conferred upon the service provider, or the designated addressee. In line with Article 13(1) of the LED, competent authorities issuing EPOs shall make available information regarding the identity of the controller, the purposes of the processing, the right to access, rectification and erasure, and information about available legal remedies. However, under the EPO proposal, information shall only be provided in the case of production orders, as preservation orders are, according to the Commission, less intrusive.[108]

2. Types of data and involvement of authorities when issuing and validating orders

The EPO proposal differentiates between subscriber data, access data, transactional data and content data.[109] EPOCs and EPOC-PRs for all data may be issued by a judge, a court, the competent prosecutor in the case concerned, or by any other competent authority as defined by the issuing State.[110] However, the Commission argues that, due to the different level of intrusiveness between subscriber data and access data on the one hand and transactional and content data on the other, different conditions for issuing EPOCs or EPOC-PRs should be applied.[111]

In line with that argument, recital 23 of the proposal determines that '[a]*ll data categories contain personal data, and are thus covered by the safeguards under the Union data protection*

[106] Article 13(3) of Directive (EU) 2016/680.
[107] Where the service provider has not already informed the data subject.
[108] COM(2018) 225 final, Strasbourg, 17.4.2018, p. 20.
[109] Under Article 2(7), (8), (9) and (10), COM(2018) 225 final, Strasbourg, 17.4.2018.
[110] Article 4(a) and (b) of the e-evidence proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.
[111] COM(2018) 225 final, Strasbourg, 17.4.2018, p. 5.

acquis, but the intensity of the impact on fundamental rights varies, in particular between subscriber data and access data on the one hand and transactional data and content data on the other hand'.

Thus, while orders to produce subscriber data or access data may be issued for all criminal offences, in case of transactional data or content data, orders are limited under Article 5(4)(a) (b) and (c) to criminal offences punishable by a sentence of at least three years or a criminal offence listed in relevant EU legislation.[112] Moreover, for EPOCs of transactional and content data, review by a court or an investigating judge is required, whereas production orders for subscriber and access data may also be issued and validated by the competent prosecutors in the Member States.[113] Preservation orders may be issued and validated by a judge, a court, the prosecutor competent in the case, or another competent national authority. For preservation orders, no differentiation is made between different types of data.[114]

The attribution of different standards to different types of data under the EPO proposal are questionable, firstly with regard to the differentiation in general, and, secondly, with regard to the case law of the CJEU. In its relevant judgments concerning data retention[115], the Court held that all data must be equally protected, but their intrusiveness depends on a case-by case analysis.

Thus, while content data might (and this is indeed debatable) be more intrusive regarding the *privacy* of persons, both types of data nevertheless require the same protection under EU data protection law (unless these data are special categories of data, in which case they require additional safeguards). Moreover the CJEU in *Tele2/Watson* held that '[traffic and location data] taken as a whole, is no less sensitive, having regard to the right to privacy, than the actual content of communications'.[116]

Consequently, the categorization into different types of data in the manner that it was done under the EPO proposal might not be fully in line with the CJEU case law.

3. Involvement of judicial authorities

Pursuant to Article 9 of the EPO proposal, the addressee of the order, thus, the service provider's legal representative, shall ensure that the requested data is transmitted directly to the issuing authority. The deadline for transmission is ten days upon receipt, or six hours in case of emergency. The proposal provides for various grounds for non-compliance with orders. Where an EPOC is incomplete, if the addressee cannot comply with its obligation because of *force majeure*, the data has been deleted, or if the order manifestly violates the Charter of Fundamental Rights of the European Union, the addressee shall inform the issuing authority and ask for clarification.[117] In such cases, the requested data shall be preserved until production is possible whether on the basis of a clarified EPOC or through other channels, such as MLA.[118]

[112] Council Framework Decision 2001/413/JHA, Directive 2011/93/EU, Directive 2013/40/EU and Directive (EU) 2017/541.
[113] Article 4 (1) and (2) of the e-evidence proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.
[114] Article 4(3) of the e-evidence proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.
[115] For instance, *Digital Rights Ireland* or *Tele2/Watson.*
[116] *Tele2/Watson* para 99.
[117] Article 9(3), (4), (5) of the e-evidence proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.
[118] Article 9(6) of the e-evidene proposal, COM(2018) 225 final, Strasbourg, 17.4.2018.

As a side note, the EPO proposal does not provide for data retention periods, and it should therefore be assumed that data will be retained in accordance with the storage limitation principle, enshrined under Article 5(1)(e) GDPR.

During all these steps, no judicial authority in the issuing Member State would be required to intervene, as would be the case for traditional MLA procedures or executing requests for judicial cooperation. Consequently, the EPO proposal endorses a problem-oriented approach, where MLA processes and the Directive on the EIO could not solve the issues relating to access to electronic evidence.

Conclusion

In a world where criminals are using modern communication techniques, timely access to electronic evidence is necessary, as stored data is prone to deletion or modification. Moreover, most investigations include a cross-border dimension and MLAT agreements are often outdated and too slow. Effective mechanisms to secure and obtain digital evidence are crucial for investigations that involve volatile data. These circumstances progressively led to a paradigm shift, away from classical mutual legal assistance towards mutual recognition in the EU, and, more recently, direct cooperation between (foreign) service providers and LEAs. Yet, it often seems as if recent initiatives to enhance such informal law enforcement access to data held by private companies follow the credo 'get access to lots of information at the lowest level of effort'. Moreover, this public-private relationship created a fragmented legal landscape and legal uncertainty, as service providers cooperate on a voluntary basis. This also means that, unless solutions are provided, states may be less and less in the position to maintain the rule of law to protect individuals and their rights in cyberspace.[119]

The most recently proposed initiatives is the EU Commission's Regulation on European Production and Preservation Orders is not a stand-alone element but follows a sequence of similar measures on different levels.

The concept of enhancing already existing direct cooperation between LEAs and service providers commenced with Article 18 of the Cybercrime Convention on production orders and Article 32 on direct access, under which requesting parties can reach beyond the traditional borders of jurisdiction in order to obtain electronic evidence. These Articles are supposed to be supplemented by an Additional Protocol. The Cybercrime Convention serves as a guideline to develop comprehensive and harmonized national legislation against cybercrime and seeks to establish a framework for international cooperation between the Parties to the Convention. However, some states participating in the Cybercrime Convention such as Canada and the U.S. are not members to the CoE Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data[120], which might cause problems in terms of data protection standards.

[119] CoE: Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention, Version 19 March 2018, p. 2.
[120] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108, Strasbourg, 28/01/1981. Cf. on the recent update of this convention: Jörg Ukrow, 'Practitioner's Corner · Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108', European Data Protection Law Review (EDPL), Volume 4 (2018), Issue 2, Page 239 – 247.

Following the *Microsoft* case, the U.S. CLOUD Act became a subsequent piece of the puzzle, causing controversies with regard to the revision of executive agreements[121], its complicated redress mechanisms and the involvement of companies like Microsoft in the lobbying of the bill. Under the CLOUD Act, it is likely that each individual EU Member State will enter into bilateral agreements, instead of one comprehensive agreement applicable to all Member States. These agreements will be based on an assessment of human rights standards in the respective country, which in the EU should (at least with regard to data protection) not create major concerns. However, where countries with rather low human rights standards can qualify for such agreements, harmonization might quickly be jeopardized and the question of reciprocity coming from other parts of the world could become a relevant challenge.

The proposal for a Regulation on European Production and Preservation Orders is (for the time being) the final piece in the puzzle, although it is not at all clear yet what the final outcome of it will be after the legislative procedure is completed. Like the U.S. CLOUD Act and the provisions under the Cybercrime Convention, the EPO proposal allows the substitution of traditional MLA procedures for international cooperation on criminal law enforcement access to data, requiring service providers to comply with production orders regardless of where the data are stored. Moreover, all three initiatives offer unilateralism and therefore create more conflicts of laws where service providers responding to orders might not be in compliance with the laws of the host country.

The extraterritorial effect of domestic production orders may thus, lead to complex issues if the relationships between the different instruments are not sufficiently well defined to prevent overlapping or contradiction. Thus, initiatives on different levels that are each applicable in their own corners may result in even more conflicts of laws than is currently the case, instead of removing the currently existing conflict of laws.

Further questions remain with regard to handing previously judicial tasks of receiving orders to preserve or produce evidence over into the hands of private companies. This may also affect the admissibility of evidence in criminal proceedings. As the ECtHR pointed out in *Gäfgen v. Germany*:

> '*As to the examination of the nature of the Convention violation found, the Court reiterates that the question whether the use as evidence of information obtained in violation of Article 8 rendered a trial as a whole unfair contrary to Article 6 has to be determined with regard to all the circumstances of the case, including respect for the applicant's defence rights and the quality and importance of the evidence in question*'.[122]

Although the initiatives are an attempt to creating a more harmonized framework for the fast gathering of electronic data (evidence), it should not be *easy* for LEAs to access and gather

[121] However, some commentators argue that the process of certification appears to be a thorough one: in particular, to qualify for an agreement the US Attorney General must determine that a candidate country's domestic law affords robust substantive and procedural protections for privacy and civil liberties, based on open criteria. See: Gavin Robinson, 'Data Protection and the European Production Order for Electronic Evidence in Criminal Matters' (Draft), May 2018.
[122] European Court of Human Rights (Grand Chamber), *Gäfgen v. Germany*, Application no. 22978/05, 1 June 2010.

evidence, as there is a risk that data may become subject to abuse. Therefore, more discussion is needed into finding the adequate balance between both interests.