ARTICLES

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

EU CRIMINAL PROCEDURAL LAW ONTO THE GLOBAL STAGE: THE E-EVIDENCE PROPOSALS AND THEIR INTERACTION WITH INTERNATIONAL DEVELOPMENTS

CHLOÉ BRIÈRE*

ABSTRACT: The evolution of information and communication technologies has impacted society, including the modus operandi of criminals, who use them in the preparation and commission of their criminal activities. This led to the adaptation in the work of criminal justice actors who increasingly rely on electronic evidence in the course of criminal proceedings. This type of evidence, composed of data, including sensitive personal data, presents certain characteristics, as it is often produced online, easily moved and destroyed. As a consequence, several actors started to develop new standards on direct cooperation with service providers for obtaining the preservation and disclosure of such data. The present *Article*, taking the perspective of the European Union in such matters, aims to analyse the mechanisms through which the EU, relying on both its internal and external competences, participates in the elaboration of common criminal procedural rules. Building on the internal EU proposals on e-evidence, the EU claimed external competences to negotiate a bilateral agreement with the United States of America and to participate in the negotiations of a Second Protocol to the Budapest Convention on Cybercrime. If at the current stage of the negotiations, it is unclear what will result of these parallel processes, the EU has the possibility in the elaboration of these standards to manifest the importance it grants to the protection of fundamental rights, both internally and externally.

* Post-Doctoral Research Fellow F.R.S-F.N.R.S., Université libre de Bruxelles, chloe.briere@ulb.be. This *Article* has been finalised in June 2020, and it does not integrate developments that occurred after that date.

EUROPEAN PAPERS
VOL. 6, 2021, NO 1, PP. 493-512
www.europeanpapers.eu
ISSN 2499-8249
doi: 10.15166/2499-8249/479

KEYWORDS: electronic evidence – cooperation in criminal matters – criminal procedural law – external relations – USA – Budapest Convention.

I. Access to electronic evidence as a new tool for criminal justice actors

Social media, webmail, messaging services and applications are nowadays increasingly used to communicate, work, socialize or obtain information. These behavioural changes have also been integrated by criminals, who have adapted their modus operandi. Beyond the rise of cybercrimes, such as identity theft or phishing, based on such technologies, criminals also use them to commit "ordinary" crimes. In such circumstances, criminal justice actors, be it law enforcement or judicial authorities, adapt to the evolution of communication and information technologies, following the evolution in the criminals' *modus operandi*. Such adaptation has been recently focussed on the necessity to be able to collect specific types of data, referred to as electronic evidence, thanks to which investigators can find leads to determine who committed a crime and obtain evidence that can be used in court.[1] This data, which can very easily be destroyed or moved includes for instance information allowing to establish the localisation of a suspect at the moment a crime was committed, or retrieving the content of messages exchanged between suspects proving their collusion. Obtaining such data requires a close and smooth collaboration with private actors, such as online services providers offering access to websites or telecommunication tools.

In the recent years, various initiatives have been launched at national, regional and international levels in order to facilitate the access of criminal justice actors to data held by online service providers and to organize their contribution to security objectives. It is interpreted as another sign of the "responsibilisation strategy" whereby the private sector is co-opted by the State in the fight against crime, something that has already taken place in the field of money laundering and countering terrorism financing.[2] In EU law, such strategy translates for instance the possibility for Europol to exchange personal data with private parties,[3] or the obligation imposed on service providers to take proactive measures to prevent dissemination of terrorist content online.[4] Of particular interest, and as the focus of this *Article*, can be highlighted the impetus in favour of the adoption

[1] Proposal COM(2018) 225 final of the European Commission of 17 April 2018 for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters.

[2] V Mitsilegas, 'Transatlantic Counterterrorism Cooperation and European Values' in E Fahey and D Curtin (eds), *A Transatlantic Community of Law, Legal Perspectives on the Relationship between the EU and US Legal Orders* (Cambridge University Press 2014) 296.

[3] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), art. 4(1)(m) and art. 26.

[4] Proposal COM(2018) 640 final of the Commission of 12 September 2018 for a Regulation on preventing the dissemination of terrorist content online.

of norms allowing criminal justice actors to request directly private actors holding relevant data to preserve and disclose it. While the United States of America, the country in which major service providers are head-quartered, has enacted specific legislation on the subject, efforts have also been initiated for the adoption of global standards, potentially taking the form of a Second Additional Protocol to the Budapest Convention on Cybercrime.[5] Meanwhile, the European Union and its Member States are not sitting still. The EU institutions engaged in an effort to facilitate the access by public authorities to personal data held by service providers, regardless of whether such access involves the crossing of EU jurisdictional borders (internal or external), through the proposal and negotiations of two EU internal instruments, known as the "e-evidence package".[6] In addition, the European Commission sought[7] and obtained mandates to enter into negotiations for the conclusion of a bilateral agreement with the USA,[8] and to participate in the negotiations of the Second Protocol to the Budapest Convention.[9]

The elaboration of these various norms pursues the objective of facilitating the preservation and disclosure of electronic evidence, yet it must do so without diluting the protection of the fundamental rights of individuals, such as the right to privacy, freedoms of expression and speech, and procedural rights in criminal proceedings. Since at the time of writing, the elaboration of these norms is far from reaching its end, the scope of our analysis is reduced, and cannot for instance include a critical examination of the level of protection guaranteed. The present paper will thus analyse the mechanisms through which the EU, relying on both its internal and external competences, participates in the elaboration of common criminal procedural rules at European and global levels. After highlighting the importance of elaborating common procedural standards at European and global levels (II), our analysis will be devoted to the appraisal of the three different processes in which the EU is currently engaged, in order to identify their synergies and

[5] Council of Europe Convention on Cybercrime, CETS n. 185, signed in Budapest on 23 November 2001.

[6] Proposal COM(2018) 640 cit.; and Proposal COM(2018) 226 final of the Commission of 17 April 2018 for a Directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

[7] Recommendation COM(2019) 70 final of the Commission of 5 February 2019 for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters; and Recommendation COM(2019) 71 final of the Commission of 5 February 2019 for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS n. 185).

[8] Decision 9114/19 of the Council of the European Union of 24 May 2019 authorizing the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters.

[9] Decision 9116/19 of the Council of the European Union of 24 May 2019 authorizing the European Commission to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime.

interconnections (III). Last, the potential limits to the EU's ambitions in the elaboration of common standards will be pinpointed (IV).

II. The importance of common procedural standards

With criminals' increasing use of information and communication technologies, criminal justice actors, be it law enforcement or judicial authorities, often require obtaining specific types of data, including sensitive personal data, in the course of their investigations and prosecutions. The relevant data is most generally held, stored and managed by private actors, such as online service providers or communication service providers. General instruments of EU law, concerning the provision of such services or the protection of personal data,[10] regulate the procedures and the duration for which they should preserve and store such data. However, when it comes to their cooperation with criminal justice actors, which takes the form of preserving and disclosing data that can later be used in criminal proceedings, the legal regime applicable is more fragmented. Service providers have themselves developed their voluntary cooperation with criminal justice authorities and may under specific procedures collaborate with them. This form of cooperation is far from being satisfactory, as it is to the detriment of legal certainty and accountability since the transparency reports published by service providers do not provide sufficient details regarding the exact extent of their cooperation with criminal justice actors.[11] In addition, some States enacted specific legislation allowing competent national authorities to request data from service providers. Yet the jurisdiction of these national authorities is determined by the principle of territoriality. While this national legislation was initially suited to address situations in which all elements are located within the same State (service provider established in State A, individual suspected of having committed an offence residing in State A and data stored in State A), their application is more complex in cases which present a cross-border element. In practice, such cross-border dimension is almost always present when the data is generated online.[12] Due to the borderless and immaterial nature of the Internet, service providers may most likely be based in another jurisdiction, and they often store the data generated by users in various distant data centres.[13] A strict legal regime would imply that national criminal justice actors do not only have to gain knowledge on the localisation of

[10] 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 (General Data Protection Regulation).

[11] S Carrera and M Stefan, 'Access to Electronic Data for Criminal Investigations Purposes in the EU' (20 February 2020) CEPS Paper www.ceps.eu 22.

[12] C Kuner, 'The Internet and the Global Reach of EU Law' in M Cremona and J Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford University Press 2019) 116.

[13] R Bismuth, 'Le Cloud Act face au projet européen e-evidence : confrontation ou coopération?' (2019) Revue Critique de Droit International Privé 683, or T Christakis, 'Données, extraterritorialité et solutions internationales aux problèmes transatlantiques d'accès aux preuves numériques' (2017) CEIS The Chertoff Group 2.

the data and the establishment of the service provider, but also to activate mechanisms for cross-border cooperation between judicial authorities in criminal matters with each State potentially concerned. Among these mechanisms, can be included mutual legal assistance treaties, being bilateral or multilateral treaties,[14] or the European Investigation Order, an instrument only applicable between authorities of EU Member States.[15] Even though these mechanisms are currently relied upon on a daily basis, they have been considered insufficiently efficient, burdensome and time-consuming, especially considering the high volume of electronic evidence to be requested.[16]

To remedy such burdensome procedures, some States have enacted legislation allowing public authorities to request such evidence directly from service providers, regardless of the localisation of the data, as long as they offer their services in their territory. Such possibility is expressly foreseen in the Budapest Convention on Cybercrime.[17] Of particular interest, the United States of America, the country in which major global online service providers are headquartered, have enacted in 2018 a specific piece of legislation, known as the Cloud Act, an acronym for *Clarifying Lawful Overseas Use of Data*.[18] This legislation had been adopted in reaction to a particular case, in which Microsoft refused to communicate data about an individual suspected in a drug trafficking case. The company argued that the data stored in Ireland was outside US jurisdiction. Obtaining the data thus required a request for mutual legal assistance addressed to the Irish authorities. The Cloud Act now forces service providers subject to US jurisdiction to preserve and disclose the content of a wire or electronic communication regardless of whether such communication is located within or outside the USA.[19] Yet such unilaterally enacted norms present several disadvantages.

The fragmentation of the applicable laws may lead to conflicting obligations, preventing or slowing down the preservation and disclosure of data. This is for instance the case when a service provider subject to US jurisdiction is compelled under the Cloud Act to disclose data but is also prohibited from disclosing it under the law of the country in which the data is stored. National legislations can indeed also provide certain restrictions to the disclosure of data, making it dependent upon the existence of dual criminality,

[14] See for instance the European Convention on mutual legal assistance of 20 April 1959, CETS n. 30, or the bilateral agreements signed by the EU, such as the Agreement between the European Union and Japan on mutual legal assistance in criminal matters [2010], or the Agreement between the European Union and Japan on mutual legal assistance in criminal matters [2003].

[15] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

[16] Europol, SIRIUS EU Digital Evidence Situation Report 2019, Cross-border access to electronic evidence, 2019.

[17] Budapest Convention, art. 18(1)(b) cit.

[18] U.S. Congress, Cloud Act, 18 U.S.C., para. 2713.

[19] D Callaway and L Determann, 'The New US Cloud Act – History, Rules and Effects' (2018) The Computer and Internet Lawyer 1, or R Bismuth, 'Every Cloud Has a Silver Lining, Une analyse contextualisée de l'extraterritorialité du Cloud Act' (2018) La Semaine Juridique, Entreprises et Affaires 35.

prohibiting the preservation and disclosure of data relating to its nationals or residents, or due to provisions on privileges or immunities. [20]

As a result of fragmentation and the deriving conflicts of laws, service providers face the risk of violating one country's law in order to comply with the law of another. The risk is even higher for those providing online services. The pluralistic and fragmented nature of Internet gives rise to even more situations where different norms cover the same actors or conducts without rules to determine which one has priority.[21] This situation also impacts individuals and the protection of their fundamental rights. There is a lack of legal certainty and clarity for users of online services, who may most certainly have difficulties in grasping what are the laws applicable to the preservation and the disclosure of the data they generate. This is particularly problematic in situations in which service providers are compelled to collaborate with criminal justice authorities. The data collected represents an important intrusion in a person's privacy, and it might end up as evidence used in court to convict an individual and impose criminal sanctions that can amount a deprivation of his/her liberty. The data collected may also be used in proceedings, which could lead to violations of freedom of expression and freedom of speech. In the light of these potential interferences with their rights, individuals shall be able to rely on safeguards. These ultimately include the rights of the defence applicable in the course of criminal proceedings and trials in the country having jurisdiction, but individuals should also be able to benefit from safeguards specific to the preservation and disclosure of personal data by service providers in the context of cross-border proceedings.

The current fragmentation resulting from unilaterally enacted norms is thus highly problematic. From a practitioner's perspective, it may impair the conduct of criminal investigations and prosecutions, especially those with a cross-border dimension. Delays in the execution of MLA requests or EIOs may lead to the disappearance of the evidence, as electronic data may easily be destroyed or hidden. The situation is also problematic from a fundamental rights' perspective. It also endangers the rights of both legal persons, such as service providers, and natural persons, depriving them of legal certainty and enforceable rights. These elements have been considered sufficient to support the elaboration of common standards, which translated into the initiation of various processes aiming at clarifying the law applicable with regard to electronic evidence.

III. The EU's contribution to the clarification of the applicable law

In order to remedy the fragmentation of the rules that allow public authorities to directly request that service providers preserve and disclose electronic evidence, a clarification of

[20] Budapest Convention, arts 27, 29 and 30; US Cloud Act, '(h) Comity Analysis and Disclosure of Information regarding Legal Process Seeking Contents of Wire or Electronic Communication', '(2) Motions to quash or modify', amending Section 2703 of title 18, United States Code.

[21] C Kuner, 'The Internet and the Global Reach of EU Law' cit. 121.

the applicable law is required. Such clarification entails not only the elaboration of common or at least compatible standards, but also the adoption of rules addressing conflicts of legislation. If there is a form of consensus on the need for such clarification, complexity increases when turning to the way such clarification is provided. Taking the perspective of the European Union, such clarification results from three intertwined processes. A first process consists in the elaboration of norms applicable to service providers operating within the EU, in order to ensure the application of uniform standards within the Union. A second process lies in the negotiation of multilateral norms, aiming at providing minimum common standards. The EU has an interest in ensuring that those standards are as much as possible compatible with the future EU law on the matter. Finally, a third process resides in the negotiation of a bilateral agreement with the USA. This agreement would complement the international standards by addressing more specifically potentially conflicting obligations between EU and US laws, and providing for more specific rules, for instance on the authorities competent for requesting evidence. The EU institutions are taking part in these three simultaneous processes that interact between each other, and they defend specific interests in each of them.

III.1. EU standards with a large territorial scope of application

Within the EU legal order, the process of elaborating norms on services providers' direct cooperation with criminal justice authorities started when the Commission published on 17 April 2018 its 'e-evidence package', a hybrid package composed of two legislative proposals belonging to different fields of EU law. The first instrument proposed consists in a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, which is based on art. 82 (1) TFEU, the legal basis at the disposal of the EU legislator for the adoption of EU instruments approximating criminal procedural law.[22] The text seeks to introduce two new mechanisms in the EU legal order, namely the European Production Order and the European Preservation Order, both issued or validated by a judicial authority and addressed directly to service providers. The latter are defined broadly and include those who provide electronic communication services, or internet domain name and IP numbering services, and those who provide "information society services", including social networks or online marketplaces.[23] The Production Order aims to request and obtain the production of different categories of data,[24] while the Preservation Order aims to prevent the removal, deletion or alteration of data in situations where it may take more time to obtain it, for instance because judicial cooperation

[22] Proposal COM(2018) 640 cit.

[23] *Ibid*. art. 2(3).

[24] The text foresees a gradation: subscriber data and access data can be requested for any criminal offence, but transactional and content data should only be requested for offences which carry a maximum custodial sentence of at least 3 years or more. The text also foresees an exception for a certain number of offences falling below that threshold but for which evidence will typically be available mostly in electronic form.

channels are used. These orders will be addressed to service providers via specific certificates, whose content is defined in annexes to the Regulation, delivered to their legal representatives. This Proposal for an EU criminal law Regulation indicates the EU's interest in exercising its competences in the matter, in order to put an end to the fragmentation of national legislation. In this field of shared competences, the Member States remain free to act as long as the EU has not decided to exercise its competence. The proposal thus marks a limit to the autonomy of the Member States, which also impacts their capacity to act externally and negotiate with external partners.

The second instrument proposed is a Directive, based on arts 53 and 62 of the TFEU, which lays down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.[25] The Commission opted for a separate internal market instrument, advancing the necessity to eliminate obstacles to the freedom to provide services, resulting from uncoordinated national solutions and potentially conflicting national obligations.[26] In substance, the text provides for measures on the legal representation in the EU of certain service providers for the purpose of gathering evidence in criminal proceedings.[27] Service providers will have to designate at least one legal representative in the Union, who shall reside or be established in one of the Member States where the service provider is established or offers services.[28]

The key feature of these two envisaged EU instruments lies in their scope of application, characterised by a broad territorial extension of the scope of EU law.[29] The envisaged texts would apply to a large group of economic operators established well beyond the geographical borders of the EU, namely those "enabling legal and natural persons in one or more Member States to use services and having a substantial connection – based on specific factual criteria - to the Member State in which the service is provided".[30] Such substantial connection shall be considered to exist where the service provider has an establishment in the EU, or in the absence of such establishment, when specific factual criteria, such as a significant number of users, or the targeting of activities in one or more

[25] Proposal COM(2018) 226 cit.

[26] *Ibid*. 4.

[27] A specific provision (art. 3(3)) deals with the consequences of variable geometry in judicial cooperation in criminal matters, and foresees that all Member States should be required to ensure that service providers not established in the Union but offering services in the Union designate a legal representative in the Union, which would be the addressee of direct requests in cross border situations and of requests based on judicial cooperation between judicial authorities.

[28] Proposal COM(2018) 226 cit. art. 3.

[29] J Scott, 'The New EU Extraterritoriality' (2014) CMLRev 1343.

[30] Proposal COM(2018) 640 cit. art. 2(4) and Preamble 7 "application should not depend on the actual location of the provider's establishment or of the data processing or storage facility". See also Proposal COM(2018) 226 cit. art. 2(3).

Member States,[31] make it possible to identify the connection with the EU.[32] Such a broad scope of application is not unique, especially for texts regulating online services. Similar provisions can be found in the GDPR,[33] or in the proposal for an e-privacy Regulation, which also foresees the appointment of legal representatives in the Union for online service providers.[34] The future provisions on the preservation and disclosure of electronic evidence will be contained in instruments addressed only to EU Member States, but the standards they contain will be applied far beyond the EU's territory. This approach, which is not questioned by the Council or the European Parliament,[35] mirrors the one taken in the US Cloud Act.[36] This is understandable and pragmatic, as a scope of application limited to the EU's territory would fail to achieve the objectives pursued by the e-evidence package.

Yet the envisaged EU standards present shortcomings. The EU is at risk of "regulatory overreaching", i.e., the risk of EU law being applied so broadly that it stands little chance of being enforced.[37] In addition, many service providers will prove to have a substantial connection with the EU, and they have greater chances of facing conflicting obligations. To resolve such conflicts, the proposal for a Regulation initially envisaged two possibilities under which a service provider could object to the execution of a European Production Order. Such objections would have applied when the order conflicted with applicable laws of a third country prohibiting the disclosure of the data concerned, either to protect the fundamental rights of the individuals concerned or the fundamental interests of the third country related to national security or defence;[38] or any other third country's rules.[39] In such circumstances, the competent court in the Member State of the issuing authority would have transmitted all relevant legal and factual information about the case to the third country's central authority. After review, the latter would have had the possibility to object to the disclosure of the data concerned, leading the competent court in the issuing country to lift the Order.[40]

[31] This entails for instance the availability of an app in the national app store, providing local advertising, advertising or customer service in the language used in that Member State, etc.

[32] General Approach 10206/19 of the Council of 11 June 2019 on a Proposal for a Regulation, Preamble 8.

[33] Art. 3(2) Regulation (EU) 2016/679 cit., see C Kuner 'The Internet and the Global Reach of EU Law' cit. 129.

[34] Proposal COM(2017) 10 final of the Commission of 10 January 2017 for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications, art. 3.

[35] Draft Report 10206/19 LIBE_PR(2019)642987 of the European Parliament on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters, no amendment on this specific point; and General Approach of the Council on a Proposal for a Regulation, art. 2(4) – addition of the requirement of specific factual criteria for establishing a substantial connection with the EU.

[36] R Bismuth, 'Le Cloud Act face au projet européen e-evidence' cit. 685.

[37] C Kuner, 'The Internet and the Global Reach of EU Law' cit. 138.

[38] Proposal COM(2018) 640 cit. art. 15

[39] *Ibid*. art. 16. For an analysis of this procedure, see R Bismuth, 'Le Cloud Act face au projet européen e-evidence' cit. 689.

[40] Proposal COM(2018) 640 cit. art. 15(6).

The Council substantially amended the text, transforming two provisions into one applicable in all cases of conflicting obligations,[41] and introducing a ten-day deadline for the addressee to inform the issuing authority.[42] These changes were criticised for reducing the influence of third country authorities and deleting the obligation of the competent court in the issuing country to dismiss the order if a conflict of laws is established.[43] The sensitivity of the issue is further reinforced with the draft European Parliament amendments. The approach proposed is radically different: as the order would no longer be transmitted to the service provider but to an executing authority, the latter would have to inform the issuing authority of a potential conflict within 10 days from the receipt of the order, via a notice including all relevant details on the law of the third country, its applicability to the case at hand and the nature of the conflicting obligation. As in traditional EU mutual recognition instruments, the executing authority would furthermore have the last word for taking a final decision on the execution of the order.[44] These elements illustrate the difficulties in determining the adequate procedure to resolve conflicting obligations, and further reinforce the importance of the two other processes in which the EU is engaged to mitigate these shortcomings.

III.2. Negotiating a bilateral agreement with the United States of America

The negotiations of a bilateral agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters with the US take place in a specific context. The US and the EU have a well-established history of cooperation in criminal matters.[45] In addition to their agreements on extradition and mutual legal assistance, they concluded in 2016 a specific agreement, known as the Umbrella Agreement on Data Protection and Privacy,[46] which provides additional standards for the protection of personal data in the course of information exchange in criminal matters.[47] Furthermore, they already cooperate in relation with the collection of electronic evidence. A direct mechanism provided for in US law allows US-based service providers to cooperate directly with European authorities, but it only covers non-content data, and it is only voluntary.[48] Lastly,

[41] General Approach 10206/19, cit. 45, deletion of art. 15.

[42] *Ibid*. 46, art. 16(2).

[43] 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

[44] Draft Report of the european Parliament cit. amendment 173, art. 14(a)(5).

[45] See the Agreement on extradition between the European Union and the United States of America, or the Agreement on mutual legal assistance between the European Union and the United States of America. For a detailed analysis of these agreements, see V Mitsilegas, 'The New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data' (2003) European Foreign Affairs Review 515.

[46] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences.

[47] These rules include notably clear limitations on data use, right to access to personal data and to rectification, notification in the case of data security breaches, and judicial redress and enforceability of rights.

[48] Recommendation COM(2019) 70 final cit. 2.

US authorities collaborate with European authorities desiring to request information held by US-based service providers thanks to the mutual legal assistance treaty (MLAT) process, under which judicial cooperation requests are issued and transmitted. This process is currently applicable to all EU Member States, with whom the US has concluded mutual legal assistance agreements, under the framework of the broader EU-US mutual legal assistance agreement which was signed in 2003 but has not yet entered into force.

In this context, the need for a new agreement on electronic evidence stems from various factors, among which the volume of requests addressed to the USA where the largest service providers have their headquarters, and the alleged difficulties arising from the length of judicial cooperation based on the EU-US mutual legal assistance treaty, under which requested evidence may be obtained in an average of 10 months.[49] Additionally, a new agreement could allow the EU to benefit from the possibility provided for in the US Cloud Act to conclude executive agreements governing access by a foreign government to electronic data held by communications- service providers in the United States.[50]

From the EU's perspective, a new agreement should pursue three objectives: 1) to address conflicts of law and set common rules for orders on content and non-content data addressed to a service provider that is subject to the law of another contracting party, such as the binding character of such order, the obligation to disclose the request to the data subject, etc.; 2) to allow for a transfer of electronic evidence directly on a reciprocal basis by a service provider to a requesting authority; and 3) to ensure respect for fundamental rights, freedoms and general principles of EU law.[51] These objectives translate in various priorities in the Commission's mandate. The agreement should set out the conditions to be met before a judicial authority can issue an order, thus excluding the issuance of orders by other public authorities. The agreement should also contain procedural right safeguards, such as the fact that data may not be requested for its use in proceedings that may lead to the death penalty, or a life imprisonment without a possibility of review and a prospect of release,[52] or specific safeguards for data protected by privileges and immunities.[53] With regard to the procedure, the negotiating mandate also refers to the importance of complying with the Umbrella Agreement on Data Protection and Privacy, and provides for additional safeguards that take into account the unique requirements of the transfer of electronic evidence directly by service providers rather than between authorities and transfers from competent authorities directly to service

[49] *Ibid*.

[50] US Cloud Act cit. Sec. 5. Executive Agreements on Access to Data by Foreign Governments, para. 2523.

[51] Recommendation COM(2019) 70 final cit. 8.

[52] These safeguards, relating to the risk of the e-evidence requested being used in proceedings leading to death penalty or life imprisonment, are not an exception. See for instance the provisions in the MLA agreements with Japan and the USA.

[53] Addendum 9666/19 of the Council to the Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters 7.

providers.[54] The EU also intends to require reciprocity in the rights and obligations of the parties, and in particular reciprocity in terms of the categories of persons whose data must not be sought pursuant to the future agreement. This refers notably to the possibility, foreseen in the Cloud Act, for the service provider to file a motion to modify or quash the legal proceedings if the provider reasonably believes that the customer or subscriber is not a US person and does not reside in the US.[55] Such restrictions should as a consequence be applicable to EU citizens and residents.[56]

The negotiations on the future EU-US bilateral agreement started on 25 September 2019, and even though two rounds of negotiation have already taken place in September and November 2019, the discussions remain rather general. Nevertheless, it is possible to analyse what could be the content of the future EU-US agreement in the light of the agreement that the US has concluded with the United Kingdom on access to electronic data for the purpose of countering serious crime,[57] the first agreement concluded under the Cloud Act a few months before the UK's withdrawal from the EU. Of particular interest are the provisions foreseeing that the orders shall be subject to review or oversight under the domestic law of the Issuing Party by a court, judge, magistrate, or other independent authority (art. 5(2)), and the issuing party's designated authority, which shall transmit the order to a service provider, must review and certify the compliance of the order with the agreement (art. 5(6) and (7)). On fundamental rights and freedoms, the agreement refers to the EU-US Umbrella agreement (art. 9), as well as to the compatibility of the agreement with the Parties' respective applicable laws on privacy and data protection (art. 9(2) or art. 10(10)). The agreement also provides for a specific procedure when a service provider wishes to raise objections about the invocation of the agreement for a specific order; including a potential conflict of laws. In such situations, the service provider's objection is to be raised successively to the Designated Authorities of the Issuing and Receiving Parties, which may confer in an effort to resolve any such objections, and meet periodically and as necessary to discuss and address any issues raised (art. 5 (11)). Whereas some provisions of the text can be considered as a precedent compatible with the red lines identified by the EU, there are still unresolved issues, in particular regarding conflicts of law. In addition, the conclusion of an UK-US agreement does not make the negotiations of an EU-US agreement a less delicate process. Whereas the US and the UK negotiated their agreement with a full knowledge of

[54] *Ibid*. 8.

[55] US Cloud Act, '(h) Comity Analysis and Disclosure of Information regarding Legal Process Seeking Contents of Wire or Electronic Communication', '(2) Motions to quash or modify', amending Section 2703 of title 18, United States Code.

[56] R Bismuth 'Le Cloud Act face au projet européen e-evidence' cit. 693.

[57] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, presented to the British Parliament on 7 October 2019. For an analysis of that agreement, see T Christakis, '21 Thoughts and Questions about the UK-US CLOUD Act Agreement' (17 October 2019) europeanlawblog.eu.

their respective domestic legislation, the EU is still in the process of elaborating its own domestic standards, making its negotiations with the US a forward-looking exercise. Moreover, even once the EU standards on electronic evidence will be adopted, the exercise will remain complex considering the diversity among the EU Member States. The future EU-US agreement might most likely have to be complemented by bilateral agreements between the US and individual EU Member States, in order to accommodate national variations in the organization of criminal justice systems, or in national standards on privacy, privileges and immunities.[58]

III.3. Intervening in international negotiations on global standards

Reducing fragmentation and incompatibilities between norms enacted at national and/or regional levels finally encompasses the elaboration of global standards on the direct cooperation of service providers with public authorities in the preservation and disclosure of electronic evidence. The participation of the EU and its Member States in such process can be explained by their mutual interest in ensuring that as many countries as possible accept global norms which are at least compatible with the EU's own standards.[59] In addition of reducing risks of conflicting obligations for service providers, and facilitating reciprocal cooperation, these global standards can also become tools for the EU's bilateral relations with third countries. Finally, should the EU succeed in "uploading" its internal norms into the international level, it would grant them hierarchical authority within the EU's legal order, reinforcing the chances of their correct and uniform implementation.[60]

International negotiations concerning the elaboration of global norms on direct cooperation between repressive authorities and service providers have been ongoing for few years. They intervene under the auspices of the Council of Europe, in which the Budapest Convention, the first multilateral binding international instrument addressing cybercrime, was elaborated. The Convention aims to eliminate or at least reduce the existence of "safe havens", and to facilitate effective cooperation between law enforcement agencies.[61] Since 2017, the Cybercrime Convention Committee, i.e. the Committee in charge of supervising the implementation of the Convention, has decided to conduct negotiations in order to prepare a Second Additional Protocol. The text envisages a series of provisions, including specific provisions allowing for direct cooperation with service providers in other jurisdic-

[58] This is furthermore the position taken by the US. See Report 13713/19 of the Council and the Commission on the second round of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 8 November 2019 3.

[59] M Cremona, 'Extending the Reach of EU Law' in M Cremona and J Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford University Press 2019) 101.

[60] *Ibid*. 107.

[61] J Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation' (2014) Monash University Law Review 701.

tions with regard to request for subscribers' information, preservation requests and emergency requests.[62] As of July 2019, the negotiations have progressed well, as there is a provisional agreement on the provisions dealing with this issue. The Committee stressed that several meetings were devoted to the discussion of their compliance with data protection and rule of law requirements, and it underlined the high complexity of drafting such provisions which need to be compatible with the systems of, and be of benefit to, all Parties of the Convention.[63]

A provisional text was agreed upon on 8 November 2019, establishing a procedure for direct cooperation between the authorities in one Party and a service provider in the territory of another Party to obtain subscriber information. The draft provision allows parties to make a declaration through they accept only orders "issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision".[64] The draft text also allows parties to require simultaneous notification of the order, and/or to require the service provider to consult their authorities in identified circumstances prior to disclosure.[65] Last, it allows the parties to instruct the service provider not to disclose the information if the disclosure may prejudice criminal investigations or proceedings in the receiving Party; or if conditions or grounds for refusal would apply had the subscriber information been sought through mutual assistance.[66] The role of the EU in the elaboration of this provisional text seems limited considering that the Commission only obtained the authorisation to participate in the negotiations on behalf of the EU in July 2019,[67] and so far has only participated in the negotiation sessions held in July and September 2019.[68]

Nevertheless, the late participation of the EU in such negotiations is crucial for several reasons. Firstly, it signals the EU's support of the Budapest Convention and its Addi-

[62] Cybercrime Convention Committee, Terms of reference for the preparation of a draft Second Additional Protocol to the Convention on Cybercrime, 9 June 2017, T-CY (2017)3, 3.

[63] Cybercrime Convention Committee, Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, State of play, 8 July 2019, T-CY (2019)19.

[64] Cybercrime Convention Committee, Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, Provisional text of provisions, 8 November 2019, T-CY (2018)23, 15.

[65] *Ibid*. 15-16.

[66] This refer to the possibility to refer to the provisions according to which "mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation" (art. 25(4) Budapest Convention) and the possibility to refuse assistance in the absence of applicable international agreements if the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or it considers that execution of the request is likely to prejudice its sovereignty, security, order public or other essential interests (art. 27(4) Budapest Convention).

[67] Decision 9116/19 of the Council authorizing the opening of negotiations cit.

[68] Non-paper from the Commission services on the state of play of the negotiations for the second additional protocol to the Budapest Convention and the negotiations for an EU-US agreement on cross-border access to electronic evidence, Council 12318/19, 2 October 2019.

tional Protocols as the instruments of choice for international cooperation on cybercrime,[69] a claim shared with the US.[70] This aspect should not be neglected, as there are currently dissensions regarding the adequate vehicle for agreeing upon global standards. In parallel to the negotiations of the Protocol, the Russian Federation made a proposal taken on in a UN General Assembly Resolution[71] to elaborate a new international treaty negotiated in the United Nations framework. The initiative has been criticized for largely duplicating the Budapest Convention, and for potentially lowering the standards for protecting fundamental rights.

Secondly, the participation of the EU in the negotiations allows it to ensure that the future global standards will contain provisions allowing for flexibility and recognition of separate agreements concluded by Contracting Parties. The EU may seek to obtain the insertion of a disconnection clause, not only allowing its Member States to apply EU standards in "internal EU cross-border cooperation", but also organising the relationship between the envisaged EU-US bilateral agreement and the future Protocol, the former taking precedence on the latter.[72] Such disconnection clauses are frequent in Council of Europe Conventions, considering that many Parties are also Member States of the EU, and they allow these States to prevent conflicts of laws.

Thirdly, the EU's participation in the negotiations allows it to establish its competence *vis-à-vis* its Member States. The EU does not possess express external competences in the field of EU criminal law, and its competence to act externally may be implied where the conclusion of an international agreement is likely to affect common rules or alter their scope (art. 216 TFEU). This may explain why the Commission waited for the publication of the e-evidence package to seek the authorisation to participate in the negotiations. Lastly, and most importantly, this participation allows the European Commission to closely monitor the elaboration of the other parts of the Second Additional Protocol, especially regarding the respect for fundamental rights. The Commission could attempt to "upload" some of the EU's standards, or at least ensure that the future text will be compatible with them, thus further reducing the risk of conflicting obligations.

These three processes reveal how the EU is taking part not only in the elaboration of EU criminal procedural norms on the direct cooperation with service providers for the collection of electronic evidence, but also in the elaboration of criminal procedural norms with a broader scope of application. At present the content of these EU, bilateral and

[69] Council of Europe, EU Statement in support of the Council of Europe Convention on Cybercrime of 15 January 2020.

[70] Press release n. 828/19 on Joint EU-US statement following the EU-US Justice and Home Affairs Ministerial Meeting, 11 December 2019.

[71] UN General Assembly, Resolution A/RES/74/247 of the of 27 December 2019, Countering the use of information and communications technologies for criminal purposes.

[72] Addendum to the Decision 9666/19 of the Council authorizing the negotiations of an EU-US agreement, 5.

multilateral norms is not finalised, which makes it difficult to evaluate whether these negotiation processes will result in compatible standards, ensuring an adequate balance between security objectives and the protection of individuals' rights. Nevertheless, these three parallel processes constitute another illustration of the interdependence between the internal and external dimensions of the EU area of criminal justice, which is particularly strong when it comes to the collection of evidence generated in a borderless online environment.

IV. The limits to the EU's ambitions

The development of new norms allowing for the direct cooperation with service providers in the preservation and disclosure of electronic evidence is not exempt of limits and critics. As a preliminary remark, it is worth noting that the need for these new norms is in itself contested. Various actors have denounced the limited evidence brought forward, for instance by the European Commission, to justify the need for new norms on the matter.[73] In a similar vein, others have stressed the potentially limited added value of the future new instruments, stressing that the existing instruments, such as the EIO, could be put to better use before considering adopting norms.[74]

The drafting of the EU standards started in April 2018, and since then the two proposals have been discussed and negotiated within the two EU co-legislators, the Council of the EU and the European Parliament. The Council has adopted its general approaches for both proposals.[75] The work within the European Parliament advanced between April 2018 and April 2019,[76] but it was interrupted due to the European elections, which took place in May 2019. The newly (re-)elected members of the European Parliament (MEPs) took back office in July 2019, and work on legislative proposals resumed progressively. Discussions are still taking place within the LIBE Committee. Draft reports were submitted in the autumn: on 24 October 2019 for the proposal for a Regulation[77] and on 11 November 2019 for the proposal for a Directive.[78] However, even though the Croatian Presidency of the Council placed emphasis on finalizing trilogue negotiations on these texts,[79] the negotiations are far from being concluded at the time of writing (May 2020), even more so with the disruption in the legislative process caused by Covid-19. Never-

[73] G González Fuster and S Vásquez Maymir, 'Cross-border Access to E-Evidence: Framing the Evidence' (2 March 2020) CEPS www.ceps.eu.

[74] S Carrera and M Stefan, 'Access to Electronic Data for Criminal Investigations Purposes in the EU' cit. 21.

[75] General Approach 10206/19 of the Council cit. and General Approach 7348/19 of the Council of 11 March 2019 on a Proposal for a Directive.

[76] European Parliament, Draft Report on the proposal for a regulation cit. Executive summary.

[77] European Parliament, Legislative Observatory oeil.secure.europarl.europa.eu.

[78] European Parliament, Legislative Observatory oeil.secure.europarl.europa.eu.

[79] Croatian Presidency, Programme, eu2020.hr, 22.

theless, the amendments introduced at this stage allow us to identify the points of convergence and divergence between the two co-legislators. Both seem to agree to substantially modify the procedure through which the European Production and Preservation Orders will be enforced. They both propose the insertion of a notification to the competent (judicial) authorities in the enforcing Member State, with a strict deadline to oppose the execution of the order, especially in light of the possible risks of violations of freedom of the press and freedom of expression.[80] MEPs also suggest the reintroduction of grounds of refusal based on fundamental rights as for the EIO,[81] a position also shared by some Member States in the Council. Both institutions also suggest introducing rules regarding the specialty principle,[82] i.e. the possibility of using the information/evidence gathered only for the purpose indicated in the order, an element not addressed in the Commission's proposal for a Regulation. These changes would allow for a certain review and examination of the order's compliance with fundamental rights prior to its execution, carried out by competent judicial authorities, rather than by the service providers themselves. However, other elements appear as potential sticking issues in the negotiations, sometimes within each institution. For example, MEPs expressed reservations concerning the choice of art. 82 TFEU for the adoption of the Regulation, considering that it focusses on the execution of law enforcement orders by private providers, and not on cooperation between judicial authorities. MEPs also expressed doubts about the choice to present a package composed of a criminal justice Regulation and an internal market Directive, the latter being considered as overreaching its goal and raising serious issues with its legal basis.[83]

The absence of a definitive (or at least a provisional) agreement on EU standards represents a difficulty for the external activities initiated by the EU. A hurdle has already appeared in the context of the negotiations of the bilateral agreement with the US. As stressed by Commissioner D. Reynders, the agreement can only be concluded by the EU once there is an agreement on internal EU rules, but the US is more than prepared to seek bilateral negotiations with EU Member States if negotiations at EU level stall or take

[80] General Approach 10206/19 of the Council cit. art. 7A and European Parliament, Draft report on the proposal for a regulation cit. amendment 141.

[81] European Parliament, Draft report on the proposal for a regulation, amendment 101 and General Approach 10206/19 of the Council cit.

[82] General Approach 10206/19 of the Council, cit. art. 12(b) and European Parliament, Draft report on the proposal for a regulation cit. amendment 465.

[83] Draft report on the proposal for a regulation of the European Parliament cit. Explanatory statement 146.

too long.[84] This may result in a fragmented patchwork of different agreements, and endanger the consistency of the EU area of criminal justice.[85] It may nevertheless be restrained by the consequences the duty of sincere cooperation has on EU Member States' external activities, especially when an EU negotiating mandate has already been agreed upon.[86] In the context of the negotiations on the Second Additional Protocol to the Budapest Convention, the agreement on the Commission's mandate is also a factor that may limit the capacity of EU Member States to act on their own. The Commission further reported working in consultation with the Council's Special Committee for the negotiations and organising on-the-spot coordination meetings for EU Member States.[87] Nevertheless the risk of disputes between the Commission and the Member States is not completely mitigated, especially in the light of previous tensions and disputes in the field of data protection and online activities that have arisen when the Commission has asserted its right to negotiate on behalf of the EU regarding a matter that was the subject of present or pending EU legislation.[88]

V. Conclusion

In response to the evolution of our societies, criminal justice authorities have stressed the importance taken in criminal proceedings by electronic evidence generated online. As it should be in democratic societies complying with the rule of law, the legislator must define the legal framework under which these authorities may request and obtain the preservation and disclosure of data, including sensitive personal data. The European Union chose within the scope of its competences to engage in three simultaneous processes for the elaboration of standards governing the collection of electronic evidence in cross-border criminal proceedings.

The proposals for EU instruments on e-evidence illustrate the challenges inherent to the elaboration of common procedural standards within the European Union, especially for the elaboration of new types of cooperation mechanisms concerning the cross-border collection of evidence. This is particularly vivid when recalling the failure of the Framework Decision on the European Evidence Warrant, never implemented and repealed in

[84] European Parliament, LIBE Committee meeting of 21 January 2020, Presentation by Didier Reynders, Commissioner for Justice on the EU-US JHA ministerial meeting of 10-11 December 2019, Agenda item LIBE/9/03307.

[85] S Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order' (2020) New Journal of European Criminal Law 10.

[86] M Cremona, 'Defending the Community Interest: the Duties of Cooperation and Compliance' in M Cremona and B de Witte (eds), *EU foreign relations law: Constitutional fundamentals* (Hart Publishing 2008) 160 ff.

[87] Report on the state of play 12318/19, 5.

[88] C Kuner, 'The Internet and the Global Reach of EU Law' cit. 119 f.

2016,[89] or when stressing the absence of initiative regarding the elaboration of common standards on the admissibility of evidence despite an explicit legal basis to do so.[90] The importance of national procedural criminal law in defining the threshold above which an evidence becomes admissible may explain the difficulties encountered in defining these future common standards.[91]

In this regard, the guarantees that will be provided for the protection of fundamental rights in the future mechanisms designed at European and international levels are essential. The proposals for EU internal instruments contain specific rules strictly framing the possibilities and modalities under which electronic evidence may be requested, including the issuance of the request by a judicial authority, or under its supervision, and disclosure of data only for offences above a certain threshold of seriousness.[92] The ongoing negotiations might even further reinforce the guarantees by granting judicial authorities in the executing States the role of reviewing the requests issued and eventually refusing their execution.[93] Similarly, the negotiation mandates obtained by the Commission stress the importance of ensuring a sufficient protection of fundamental rights, which might result in the insertion of specific clauses in the future envisaged agreements. Yet the adoption of these procedural safeguards will be a delicate task. The diversity within the EU and beyond will have to be accommodated and be reflected in the procedural rules applicable to the collection of electronic evidence. Preventing conflicts of laws will be essential in order to provide legal certainty and accessibility of the law applicable, which is of core importance, not only for service providers who should avoid being placed in a situation in which they breach either their domestic law, or EU law, but also for the protection of the rights of individuals from which they may benefit under the law of a third country or EU law.

In this context, the discussions around the procedure under which the request to preserve and disclose data will be reviewed and executed are essential to guarantee the long-term implementation of the future standards. There will be little interest in designing mechanisms that lead to decisions of inadmissibility and prevent the use of key data as evidence before courts. This concern applies to EU internal negotiations, but also to the two other processes in which the EU is currently engaged. When negotiating its bilateral agreement with the US and the future global instrument on the matter, the EU must be careful in ensuring that the facilitation of cross-border collection of evidence directly from service providers is not achieved at the expense of the protection of procedural

[89] 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.

[90] Art. 82(2) TFEU. A Weyembergh and E Sellier (30 August 2018) 'Criminal procedural laws across the European Union' www.europarl.europa.eu 62.

[91] A Weyembergh and E Sellier, Criminal procedural laws across the European Union cit. 48-52.

[92] Proposal COM(2018) 640 cit. arts 3(2), 4 and 5(4), and the amendments suggested by the Council and the Parliament.

[93] Draft Report on the proposal for a regulation of the European Parliament cit. 145.

safeguards, which are key to ensure the future admissibility of the data collected as evidence. It will also be a test of its capacity to ensure the consistency between the internal and external dimensions of the EU area of criminal justice, and the promotion of human rights and fundamental freedoms on the international stage.