ERA Forum (2019) 19:307–312
https://doi.org/10.1007/s12027-018-0525-4

EDITORIAL

The genesis of the European Union's new proposed legal instrument(s) on e-evidence

Towards the EU Production and Preservation Orders

Laviero Buono[1]

Published online: 3 September 2018

1 Introduction

When a crime is committed, law enforcers and judicial authorities, in the framework of criminal proceedings, may need to rely on information generated, distributed or stored on electronic devices. Examples of digital devices include the following: computers, storage devices, memory cards, mobile (smart)phones, digital cameras and wearable technology (smart watches and e-bracelets). Such devices create many opportunities for the commission of crimes, such as phishing, identity theft and internet fraud among many others. Electronic information is often relevant in proving or disproving a fact or point in question relating to the guilt or innocence of the accused and, as such, the information forms part of the totality of evidence before the court. This information constitutes electronic evidence.

Within the European Union (EU), the legal framework for obtaining cross-border access to evidence was the 2000 Convention on Mutual Assistance in Criminal Matters between the EU Member States.[1] The Convention has been replaced by the Directive on the European Investigation Order (EIO) in criminal matters,[2] which,

[1] 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 [2000] OJ C 197/1.

[2] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L 130/1.

✉ L. Buono
LBuono@era.int

[1] Head of Section, European Criminal Law, ERA, Trier, Germany

based on mutual recognition, needed to be transposed by 22 May 2017. This Directive involves direct communication between judicial authorities, provides for deadlines, standardises forms and limits the possibility to refuse the execution of requests. However, requests still require some time to be processed. Especially for electronic evidence, which is volatile in nature and can be transmitted, altered or deleted easily, mutual legal assistance proceedings are considered unsuitable.

Hence, to date, in the field of electronic evidence, there is no EU *ad hoc* legislation, policy or instrument, that can be referred to or used by legal practitioners and, since computer artefacts can be modified and overwritten, that poses challenges where sources of electronic information must be authenticated and verified. Within the EU, evidence rules vary considerably between jurisdictions, even amongst countries with similar legal traditions. In general terms, however, legal systems of the common law tradition tend to have defined rules as to the admissibility of evidence. In legal systems of the continental law tradition, in which professional judges retain a high degree of control over the court proceedings, admissibility of evidence may be flexible, although the weighing of evidence (including ascertaining its credibility and authenticity) can also obey a comprehensive set of rules.

2 The recent European Union's efforts to forge a comprehensive policy on e-evidence

For the past years, important steps were taken at European level to develop an adequate legal framework to address the challenges posed by the gathering of e-evidence.

Already in 2013, the Council of Europe published the 'Electronic evidence guide—A basic guide for police officers, prosecutors and judges'. This guide was developed within the framework of the EU and the Council of Europe joint project CyberCrime@IPA. Page 157 of the guide states: *'There are an increasing number of cases involving electronic evidence stored on computer systems or other devices. Judges* (*like prosecutors and investigators*) *must be prepared to deal with cybercrime and electronic evidence. In most cases, judges* (*like prosecutors and investigators*) *encounter difficulties in coping with the new realities of the cyber world and need to be trained in the knowledge and understanding of cybercrime and electronic evidence'*.[3]

Within the EU, in January 2014, the European Anti-Fraud Office (OLAF) issued the 'Guidelines on digital forensic procedures for OLAF Staff'.[4] At national level, a set of guidelines dealing with electronic evidence gathering is the 'Good practice guide for computer-based electronic evidence—Version 3.0' published in the United Kingdom by the Association of Chief Police Officers (ACPO).[5] In 2014, the EU Agency for Network and Information Security (ENISA) published the 'Electronic evidence—a basic guide for first responders'. In the manual, on page 8 it is stated:

[3]For more information on the CoE e-evidence guide (intended for use by law enforcement and judicial authorities only) and other CoE's training material on cybercrime consult this page: https://www.coe.int/en/web/cybercrime/trainings.

[4]Available here: https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf.

[5]ACPO Good Practice Guide, available here: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

'*Proper training is a very important prerequisite for the success of the search and seizure of electronic evidence*'.[6]

In April 2015, the EU underlined in its Communication 'EU Agenda on Security'[7] possible solutions to allow for timely access to electronic evidence. The Communication noted that: '*Cyber criminality requires competent judicial authorities to rethink the way they cooperate within their jurisdiction and applicable law to ensure swifter cross-border access to evidence and information, taking into account current and future technological developments such as cloud computing and Internet of Things. Gathering electronic evidence in real time from other jurisdictions on issues like owners of IP addresses or other e-evidence, and ensuring its admissibility in court, are key issues*' (emphasis added). The Commission's commitment was supported by the Council of the EU which adopted, on 9 June 2016, its Conclusions on 'Improving criminal justice in the cyberspace'[8] calling on the Commission to take actions to improve cooperation with service providers, make mutual legal assistance more efficient and propose solutions to the problems of determining and enforcing jurisdiction in cyberspace. As a consequence, an expert consultation process, including a detailed questionnaire, was launched in July 2017.[9] The questionnaire revealed that there was no common approach to obtain cross-border access to electronic evidence for which each Member State had developed its own domestic practice.[10] There is a diversity of approaches, mainly due to the lack of a common legal framework on obtaining e-evidence, which creates legal uncertainty and clear obstacles to cross-border investigations. As a result, a detailed technical document, although not adopted or endorsed by the European Commission, was presented in 2017.[11] It was this document that laid down the foundation of the European Production Order. In fact, as possible measure, the document stated: '*A common framework across Member States could provide a basis for and recognise the legality of the current practices of direct cooperation, i.e. providing law enforcement and judicial authorities with the competence to make non-binding production requests for cross-border access to electronic evidence, and allowing service providers to disclose electronic evidence to foreign authorities on*

[6]The ENISA basic e-evidence guide, available here: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders.

[7]Communication from the Commission to the European Parliament, the Council, the European Economic and Committee of the Regions—The European Agenda on Security (Strasbourg, 28.4.2015 COM (2015) 185 final).

[8]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.

[9]Available here: https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en.

[10]On this point see the: 'Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace', p. 4 (Brussels, 7.12.2016 15072/1/16 REV1), available here: http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf.

[11]Technical Document: 'Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace', available here: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf.

the basis of such a production request, without passing through local law enforcement or judicial authorities'.[12]

As final preparatory paper, the European Commission issued in April 2018 an Impact Assessment[13] where it emerged clearly that in cross-border cases authorities have to rely on one of three channels: judicial cooperation between public authorities (often too slow), direct cooperation between public authorities and a service provider (often cumbersome and not transparent) and direct access to e-evidence (where legal frameworks remain fragmented).[14] The document also indicated that although the EIO, in application since May 2017, covers the gathering and transfer of evidence between Member States and makes Mutual Legal Assistance (MLA) procedures faster, it is still considered insufficient, slow and therefore ineffective by national experts for accessing e-evidence in criminal investigations.[15] Therefore, in the absence of EU intervention, the e-evidence gathering problem could only have been exacerbated by long time-consuming MLA requests and insufficient public-private cooperation between service providers and public authorities.

3 The 2018 EU proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters

On 17 April 2018, the European Commission proposed new rules to better equip law enforcers and judicial authorities. As a matter of fact, the EIO and the MLA procedures will continue to exist, but there will be new avenues, or 'fast tracks' for the specific case of electronic evidence.

The new legal framework that builds upon the provisions of the EIO, which effectively provides assistance between law enforcement and judicial authorities in different EU Member States, will complement it by creating a set of clear and coherent principles to enable requests by law enforcement and judicial authorities in one Member State to be made directly to a service provider in another Member State for the disclosure of data. This new set of rules consists of two proposals: 1) the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters[16] and 2) the Proposal for a Directive laying down har-

[12] Idem, p. 20.

[13] Commission Staff Working Document, Impact Assessment, Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and 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' (Brussels, 17.4.2018 SWD (2018) 118 final).

[14] Idem, p. 9.

[15] Idem, p. 23.

[16] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (Strasbourg, 17.04.2018 COM (2018) 225 final).

monised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.[17]

In a nutshell, the European Production Order will allow a judicial authority in one Member State to request electronic evidence directly from a service provider offering services in the EU and established or represented in another Member State, regardless of the location of the data. The service providers will be obliged to respond within 10 days and within 6 hours in cases of emergency. This measure will be complemented by the European Preservation Order, which under the same conditions outlined above, will oblige service providers to preserve specific data to enable the authority to request this information later via MLA, EIO or a European Preservation Order.

In light of these obligations it is important to ensure that all service providers offering services in the EU are subject to the same constraints, hence the proposal of the Directive which requires them to appoint a legal representative in the EU for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities for the purpose of gathering evidence in criminal proceedings. The new proposed Orders contain strong safeguards to guarantee privacy and the right to judicial redress. In fact, issuing these Orders will only be possible in the context of criminal proceedings with the new rules establishing an obligation for authorities to obtain approval from a judicial authority which will check the legality, necessity and proportionality of the Orders. Moreover, Production Orders to produce transactional (source and destination of a message, data on the location of the device) or content data (text, voice, etc.) are limited in the framework of criminal offences punishable in the issuing State by a maximum sentence of at least three years, or for specific cybercrimes and terrorist-related crimes defined in the proposal. Therefore, among the safeguards can be listed the following: the Orders must be approved by the judicial authority, individuals will be notified that their data was requested, they will be informed of their rights and criminal law procedural rights apply.

4 Conclusions

In the EU, concerns about the problem of obtaining electronic evidence across borders have been raised for a long time. However, it was in 2015 with the European Agenda on Security and later, in June 2016, when the EU Commission set up an expert consultation process, involving various stakeholders including service providers, practitioners and the civil society, that electronic evidence gathered momentum. Different options were envisaged that ranged from an improvement of the mutual legal assistance procedures up to brand new legislative solutions, including the enhancement of cooperation with the service providers. With the support of a large majority of EU Member States, the Council requested the Commission's legislative proposals to be tabled by early 2018.

[17] 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 (Strasbourg, 17.04.2018 COM (2018) 226 final).

There is little doubt that within a clear legal framework that defines the limits and safeguards governing the modalities under which public authorities may lawfully obtain data the overall judicial system will benefit in terms of efficiency and deliverability. With the traditional regime of MLA, originally designed for gathering physical evidence abroad, constantly under stress in today's digital environment and often impracticable, both, the public and the private sector strongly called for such a new framework. The lengthy process to finally receive or access evidence through judicial cooperation was marked as the most common complication by practitioners from law enforcement and judicial authorities.[18] To this extent, the EU's proposed initiative on e-evidence aiming at achieving a higher degree of legal certainty will certainly allow for a more time and cost-efficient way to administer justice. The fact that it will be mandatory for service providers to produce e-evidence is a clear step ahead compared to the existing voluntary cooperation, which creates challenges for service providers seeking to comply with law enforcement requests. Indeed, at present, the service providers seem to spend a lot of time and financial resources in contacting the issuing authorities in order to obtain further information on the requested data.[19]

The ball has been thrown and the adoption of the proposed new legislation is expected in spring 2019.

[18] See p. 1 of the 'Summary Report of the public consultation on improving cross-border access to electronic evidence in criminal matters', available here: https://ec.europa.eu/info/files/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en. Last accessed, 25 June 2018.

[19] Idem, p. 2.