European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

11.3.2019

4th WORKING DOCUMENT (A)

on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Relation with third country law

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Birgit Sippel
Co-Author: Sophie in't Veld

Introduction

This working document covers the relation of the proposed European Production Orders (EPOCs) and European Preservation Orders (EPOC-PRs) with third country law. It will first discuss the current way of dealing with extraterritorial requests through Mutual Legal Assistance Treaties (MLATs). Second, it will also present first considerations regarding the US CLOUD Act, the negotiating directives that the Commission published on an EU-US agreement on access to electronic evidence, and the potential consequences to the proposed e-evidence instrument. Finally, it will assess the proposed Articles 15 and 16 of the Commission Proposal for a Regulation, outlining a review procedure foreseen for cases of conflicting obligations based on fundamental rights or fundamental interests of a third country (Article 15) and other grounds (Article 16). And it will also outline the Parliament's considerations with regard to the new Article 16 as proposed in the Council General Approach from December 2018.

Mutual Legal Assistance Treaties (MLATs)

The current system of gathering and exchange of electronic information between EU Member States and third countries is based on mutual legal assistance, either on an *ad hoc* basis, a more formally established bilateral basis, or in the framework of international agreements (such as the Council of Europe (CoE) European Convention on Mutual Assistance in Criminal Matters or the CoE Convention on Cybercrime (so-called Budapest Convention)), or based on agreements the EU concluded with third states (like US or Japan).

Currently, the majority of data seems to be exchanged between the EU and the US. Therefore, this paper will concentrate on the existing Agreement on mutual legal assistance between the European Union and the United States of America (EU-US MLA Agreement), which was signed in 2003 and entered into force in 2010. This Agreement as such shall be applied in addition to the bilateral MLA agreements the Member States had concluded with the US[1]. Where such a bilateral MLA agreement does not exist, the EU-US MLA Agreement shall be applied directly to MLA issues.[2] The scope of the agreement is not limited to criminal law as such, but covers administrative proceedings regarding "investigating conduct with a view to a criminal prosecution of the conduct" as well.[3] However, the instrument is limited only to cooperation and mutual legal assistance between state authorities. Private parties are explicitly

[1] Its provisions are superseding certain bilateral provisions, namely as regards joint investigative teams, hearing by video-conference, expedited means of communication, assistance to administrative authorities, limitations of use of information, confidentiality (Article 3(1) of the EU-US MLA Agreement).

[2] See Article 3(2) of the US-EU MLA Agreement.

[3] Article 8 EU-US MLA Agreement. Such an extension is also part of existing internal EU mutual recognition instruments on gathering of evidence, for example Article 4(b) of Directive 2014/41/EU ("in proceedings brought by administrative authorities in respect of acts which are punishable under the national law of the issuing State by virtue of being infringements of the rules of law and where the decision may give rise to proceedings before a court having jurisdiction, in particular, in criminal matters"). Such provisions are being used in EU law on gathering evidence in criminal proceedings since the Schengen Implementing Convention, over the 2000 EU MLA Convention, the European Evidence Warrant till the mentioned European Investigation Order. However, such provisions are also problematic as they extend criminal law procedures to administrative authorities (with another level of guarantees and safeguards). This is clearly shown by a divergence between internal EU mutual recognition instruments, on one side (including also a possible administrative criminal phase), and internal EU harmonisation directives on procedural rights (applying only at the phase of a criminal procedure), on the other side.

excluded from its remit.[4] The EU-US MLA Agreement contains specific provisions on identification of bank information,[5] joint investigative teams,[6] video conferencing,[7] expedited transmission of requests,[8] MLA to administrative authorities,[9] limitations on use,[10] and also requests for confidentiality[11].

The Agreement allows for the requested state to impose additional conditions in a particular case and to require the requesting state to give information on how the evidence or information was used. However, generic restrictions with regard to the legal standards of the requesting State for processing personal data may not be imposed by the requested State.[12] According to the Explanatory Note to the Agreement, this means that *"refusal of assistance on data protection grounds may be invoked only in exceptional cases[...]if , upon balancing the important interests involved in a particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting State would raise difficulties so fundamental as to be considered by the requested State to fall within the essential interests grounds for refusal. A broad, categorical, or systematic application of data protection principles by the requested State to refuse cooperation is therefore precluded. Thus, the fact the requesting and requested States have different systems of protecting the privacy [...] or have different means of protecting personal data ([...], may as such not be imposed as an additional conditions under Article 9(2)."*[13]

In addition, as regards refusal grounds (except the exception on prohibition of generic data protection reservations and the prohibition of invoking a bank secrecy claim), Article 13 ("Non-derogation") states that the refusal grounds pursuant to a bilateral mutual legal assistance treaties apply. In other words, in the absence of a treaty, applicable legal principles apply as a refusal ground, including where execution of the request would prejudice its sovereignty, security, *ordre public* or other essential interests.

Looking at the effectiveness of the mentioned Agreement, the 2016 Commission review indicates that the agreement is quite useful and successful.[14] However, depending on the

[4] Article 3(5) of the EU-US MLA Agreement.
[5] Article 4 of the EU-US MLA Agreement. Compare with US FATCA law (based also on extra-territorial effects) requiring all non-U.S. ('foreign') financial institutions to search their records for customers with indicia of 'U.S.-person' status and report to US authorities.
[6] Article 5 of the EU-US MLA Agreement. Through such teams also e-evidence can be acquired in a more easy way. Where the joint investigative team needs investigative measures to be taken in one of the States setting up the team, a member of the team of that State may request its own competent authorities to take those measures without the other State(s) having to submit an MLA request. The required legal standard for obtaining the measure in that State shall be the standard applicable to its domestic investigative activities.
[7] Article 6 of the EU-US MLA Agreement.
[8] Article 7 of the EU-US MLA Agreement.
[9] Article 8 of the EU-US MLA Agreement.
[10] Article 9 of the EU-US MLA Agreement.
[11] Article 10 of the EU-US MLA Agreement.
[12] Article 9(2) of the EU-US MLA Agreement.
[13] However, this has to be seen in light of the later adopted 2016 EU-US Agreement on personal data protection ("Umbrella Agreement").
[14] Based on the 2016 Commission review as foreseen in Article 17 of the Agreement. See Outcome report, Seminar on the application of the Mutual Legal Assistance and extradition agreements between the European union and the United States of America, Council doc. 9519/16, Annex 3 (responses by 18 member states to the Commission questionnaire). There is more outgoing requests from the EU to the US than vice versa. See also EU-US relations, Review of the 2010 EU-US MLA Agreement, Council doc. 9291/16. The US records show the

individual Member State, there seems to be notable variations in the level of requests.[15] Further, even though the number of requests, mentioned in the Commission review, cover all types of requests issued under the US-EU MLA Agreement, a very significant proportion of the requests seem to be on e-evidence.[16]

As regards e-evidence, due to the US standards of probable cause, as well as the need for a court authorisation for access to content data in the US, requests for content data necessarily have to be issued via MLA. In line with this, probable cause also seems to be one of the main reasons on the US side to reject incoming requests for content data, followed by issues of proportionality (*de minimis* rule - refusing trivial offences) and freedom of speech.

However, for transactional (traffic) data, as well as subscriber and access data (including IP addresses), which can already be gathered in the US on the basis of administrative subpoenas, the standard of probable cause is not necessary and therefore not a reason for rejecting incoming requests.[17] The successful gathering and exchange of data via MLA is further supported by Eurojust, which proved to be useful in the past assistance with MLA requests between the EU and the US.[18]

Regarding the last two categories, subscriber and access data (including IP addresses), it has to be mentioned that they can be directly requested from the US service providers based on an EU law-enforcement request,[19] meaning that an MLA request for these categories would only become necessary if the operator would decline to cooperate on a voluntary basis. However, it seems that there are certain well-established channels and procedures in place for such cooperation between big US operators and EU Member States[20], with appropriate safeguards, so that subsequent MLA requests are rarely necessary.

---

opening of slightly over 7000 files as regards incoming MLA requests from EU Member States (for all kinds of evidence) for 2010-2014 (mostly from Greece, Netherlands, UK, Spain and Poland). The US, on the other side, send for the same period ca. 2000 requests (mostly to the Netherlands, Germany, UK and France).

[15] See also CEPS, Access to Electronic Data by Third-Country Law enforcement Authorities, 2015, pp. 66-67. For the period 2010-2012 a number of ca 3500 requests (for all kinds of measures, not only e-evidence).

[16] See EU-US relations, Review of the 2010 EU-US MLA Agreement, Council doc. 9291/16, p. 6.

[17] See Outcome report, Seminar on the application of the Mutual Legal Assistance and extradition agreements between the European union and the United States of America, Council doc. 9519/16, p. 2.

[18] Especially taking into account the US liaison officer at Eurojust and the US-Eurojust cooperation agreement.

[19] However, some EU Member States raised the issue about possible problems with their national legislation as regards admissibility of evidence. It is not totally clear what those problems could be, taking into account that the national authorisation procedure for the data has to be followed, like prosecutorial/court authorisation or limitations according to their own national law. Also under EU law, Article 39 of Directive 2016/680 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 ("Police Directive|") transfers to private entities (for example a US provider) of requests containing personal data are possible under certain conditions.

[20] See, for example, very detailed Apple Legal Process Guidelines for Government and Law Enforcement outside the United States with exact contact details and procedures (https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf). They address preservation (for example, a possible preservation deadline of 90 days to be extended once), emergency procedures and information requests (such as MLA requests for non-content data), detailed rules on iCloud (subscriber info and mail logs), etc. In addition, data from Microsoft, for example, shows that most EU states request non-content data only to a large extent and for most of the Member States the rejection rate is quite low (for example, for the first half of 2018 the average rejection rate for EU States was 23% ranging from 3% Luxembourg to 65% for Greece). See under https://www.microsoft.com/en-us/corporate-responsibility/lerr. See also information to direct requests to Google under https://support.google.com/transparencyreport/answer/7381738?hl=en&ref_topic=7380433.

Consequently, the need for any new instruments for subscriber, access and transactional data, at least when the big US providers are concerned, seems questionable. Even though, this may be different for requests on content data, the US authorities themselves warned that incoming EU MLA requests for content data were sometimes unnecessary for the actual prosecution of the mentioned offence.[21] Furthermore, mutual legal assistance with the US could already be improved by applying the measures foreseen in the Agreement better. With the help of joint investigation teams, possible under Article 5 of the Agreement, national Members of such teams can request measures according to their national system. Article 7 of the Agreement further allows for expedited transmission requests, meaning the use of expedited means of communications, such as e-mail and fax, with a formal confirmation ex post facto.

The Commission has pointed out that that current judicial cooperation via mutual legal assistance, including with the US, takes an average of 10 months and can entail a disproportionate expense of resources.[22] Nevertheless, in the 2016 recommendations on the Agreement[23], inter alia, better education of staff working on MLA issues, issuing of guidelines (US issued specific guidelines and a handbook exists[24]), and additional financing[25] have been highlighted as central matters for improvement and for speeding up the process. The question therefore arises whether new instruments for direct access to electronic evidence are necessary before addressing the current practice in judicial cooperation. In other words: Does the problem lie in a lack of an instrument or with the service providers who do not provide the requested data quickly enough for the investigation? Or does the problem lie in the fact that national judicial authorities are too slow in handling the requests by the demanding the national judicial authorities? If national governments provide more financial, human and technical resources to the judicial authorities handling MLA requests, electronic evidence can be provided in a more time-efficient way. The need for additional instruments, whereby one side of the national authorities involved are simply removed from the process, would then become less pressing.

When it comes to the requests on e-evidence, the review further recommended thinking about putting in place different approaches according to different data categories, including introducing clearer proceedings for emergency cases.[26]

---

[21] See Outcome report, Seminar on the application of the Mutual Legal Assistance and extradition agreements between the European union and the United States of America, Council doc. 9519/16, p. 3: *"The US participants noted that content data often seemed to be requested by default in MLA requests from EU Member States and drew the attention to the fact that transactional data, in particular. could often provide sufficient information for the purposes of investigations. Therefore, it would be beneficial to carefully assess whether content data is really necessary, or if non-content data would be sufficient, before issuing MLA requests."*

[22] COM(2019) 70

[23] Council doc. 9291/16, pp. 15-20.

[24] See, for example, Council doc. 8024/11.

[25] See, for example the 2017 Commission call for proposals with a total budget of 1 million EUR for improving cooperation between judicial authorities of EU Members States and US judicial authorities and US based service providers (under the Partnership Instrument Annual Action Programme 2016).

[26] Ibid, p. 19: *"There has been an informal practice of the provision, by the US, of electronic evidence (including content data) in emergency cases such as those involving imminent risk of serious injury or death, including in terrorism cases. The usual process is that EU Member States' law enforcement authorities liase with the US authorities who, in turn, facilitate the voluntary provision by ISPs of the required material pursuant to US law. This arrangement has worked very well and, in the most exceptionally serious and urgent cases, the US has assisted in the obtaining of evidence in under 24 hours. Under US law, such voluntary disclosure in emergency situations is accomplished without the need to meet the probable cause test."*

US CLOUD Act

1. Presentation of the law

The 2018 US CLOUD Act (US Clarifying Lawful Overseas Use of Data Act)[27] amended the Electronic Communications Privacy Act (ECPA) regulating the terms of government access and the disclosure by companies of electronic communications. The CLOUD Act was enacted mainly due to the controversy in the US v. Microsoft case[28] concerning Section 2703 of the Stored Communications Act (Title II of ECPA) regarding the question of whether or not the ECPA authorised US law enforcement to compel a provider to turn over communication content data stored outside the US (in the concrete case, emails stored in Ireland). As such, the CLOUD Act only affects historical (stored) data and does not apply to real time interceptions. However, the envisaged executive agreements (see below) could include such a possibility.[29]

The CLOUD Act introduced two important changes to this Act. In Part I, the Cloud Act adds §2713 which states that "*a provider of electronic communication service or remote computing service shall comply with the obligations of this chapter, namely to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States*". Consequently, with the CLOUD Act, any US law enforcement agency is able to access content data stored or collected outside of the United States, from service providers that are subject to jurisdiction of the United States. All service providers, including non-American, that have an office in the United States are bound by the CLOUD Act.

[27] H.R.1625.
[28] United States v. Microsoft Corp., 138 S.Ct. 1186, 1187 (2018).
[29] See J. Daskal, Setting the record straight: The Cloud Act and the reach of wiretapping authority under US law, CBDF, 2018.