EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters

19/10/2018

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 45 countries, and through them more than 1 million European lawyers. The CCBE regularly responds on behalf of its members on policy issues which affect European citizens and lawyers.

On 14 April 2018, the European Commission published a proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters.

The CCBE welcomes that the Commission took into account various aspects which the CCBE suggested during the preceding consultation process. The CCBE previously issued preliminary comments on the subject which can be consulted for more details[1]. With this paper, the CCBE wishes to further develop its position in relation to a number of aspects of the proposal.

1. Legal basis, necessity and proportionality

The key question arising from this legislative initiative is whether Article 82 (1) of the Treaty on the Functioning of the European Union (TFEU) constitutes the appropriate legal basis for an instrument enabling law enforcement authorities of a Member State to oblige undertakings offering electronic communications and/or information society services in the EU to preserve and/or produce electronic evidence, irrespective in which jurisdiction that undertaking is based and where the data are stored.

The principle of mutual recognition referred to in Art. 82 TFEU is usually understood to be reserved for cooperation between judicial authorities only. The envisaged proposal, however, does not involve the police or judicial authorities of the Member State in which is situated the undertaking in receipt of the request. Instead, the proposal seeks to confer extraterritorial jurisdiction on the police or judicial authorities of one Member State directly to address a private entity in another Member State. Moreover, the proposed regulation also involves the cross-border execution of EPOC[2]'s and EPOC-PR[3]'s that have been issued and validated by prosecutors alone and are therefore not judicial decisions

In view of these circumstances, the CCBE considers that it is not possible on the stated legal basis for the EU institutions to adopt a legal instrument enabling national authorities in one Member State to order the production of electronic evidence to private entities in another jurisdiction. It is also doubtful whether the selected legal basis suffices to adopt draft Article 13 of the proposal which obliges the Member State to provide for pecuniary sanctions for violations of the obligations under Articles 9-11.

The CCBE also considers that the choice of a Regulation instead of a Directive as the legal instrument might lead to a paradigm shift in the criminal law area which involves a high risk that higher national standards could be lowered by EU legislation. In this regard it is also relevant to note that measures concerning procedural

[1] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20180629_CCBE-Preliminary-comments-on-the-Commission-proposal-for-a-Regulation-on-European-Production-and-Preservation-Orders-for-electronic-evidence-in-criminal-matters.pdf

[2] **EPOC** stands for 'European Production Order Certificate'.

[3] **EPOC-PR** stands for 'European Preservation Order Certificate'.

harmonisation to facilitate, inter alia, mutual admissibility of evidence between Member States, may, according to Article 82 (2), be adopted only by means of directives.

Another important question is to what extent the proposal is of any added value compared to existing Mutual Legal Assistance Treaties (MLAT's) as well as the European Investigation Order (EIO) and whether it is coupled with sufficient safeguards. In other words, is the envisaged instrument really necessary to achieve its aim and proportionate to the objective it purports to achieve?

From the explanatory memorandum it seems that the main objective of the proposal is to make the securing and gathering of electronic evidence stored in another jurisdiction faster by circumventing (often under-resourced) national judicial authorities in the Member State where the evidence is stored. As such the proposal essentially introduces a mechanism through which the established systems of judicial assistance are bypassed and the protection of fundamental rights is delegated partly or in full to private parties. The CCBE strongly disagrees with this approach as it undermines the essential duties of national judicial authorities to ensure that the rights of its citizens are not compromised or undermined. Such undermining does arise, by reason that it would be no longer possible for national judicial authorities to undertake a legality check of requests for judicial cooperation emanating from the authority of another Member State. Hence, the CCBE considers that, instead of curtailing the role and responsibilities of national judicial authorities, a more appropriate approach would be to make MLA and EIO procedures faster through digitisation and by better equipping national authorities to respond to cross-border requests. Without some form of legality check by the relevant judicial authorities of the member state in which the undertaking is situated, there is a risk that the undertaking may be required to make disclosure of a nature which could not normally be required in the jurisdiction where the data are sought. Smaller entities may lack the legal resources and expertise to query the legality of the production order.

In addition to the need for a legality check of the production order by the relevant judicial authorities of the country where the data are sought, there might also be a need for the participation in the proceedings of a person or entity that is aware of matters such as whether the evidence is likely to be covered by lawyer-client confidentiality. Normally that would be the data controller (e.g. law firm). It is appreciated that this might not always be appropriate, especially where there is a risk of destruction of the evidence. However, once the data have been secured, it would be possible and appropriate to conduct a legality check prior to the production of the targeted data.

The CCBE therefore proposes to restrict the scope of the proposal so as to relate to preservation orders only. For the production of electronic evidence, a preservation order could be followed up with the launching of a European Investigation Order or with a procedure under a Mutual Legal Assistance treaty. Another argument in favour of restricting the proposal to preservation orders is the procedural and technical uncertainties regarding the execution of production orders addressed to private entities in another jurisdiction without the involvement of the authorities where the data are sought, including:

- How should EPOC's be served to addressees (by registered post, electronically, special delivery system etc.)?
- How are addressees expected to submit the requested data to the issuing authority (means, formats, structure, size limits etc.)?
- How can the security of the transaction be guaranteed to ensure that the data are true, accurate and untampered with?
- How can addressees evaluate the authenticity and legality of the EPOC's?

In consequence of the issues highlighted above, the CCBE submits that the proposal should be restricted in its scope to European Preservation Orders and that the objectives pursued by the Commission could be equally attained by using, in combination with the creation of a European Preservation Order, the procedures provided for under the EIO and MLAT's which, in consequence, might also require improvement.

Nevertheless, in the event that the European Institutions were to decide to go forward with the proposal as it stands at present, the CCBE would set out some further observations and suggestions for amendment of the proposal which are set out below.

2. Judicial review in the executing Member State

Some form of judicial review in the executing State would be necessary in order to ensure sufficient protection of fundamental rights. The CCBE therefore suggests that there be used the provisions of Article 11(1) of the EIO Directive 2014/41 on the grounds for non-recognition or non-execution of the order. If it jeopardises the investigations to notify the data subject before the data are handed over, at least a meaningful judicial review must be performed in the executing Member State on the legality of the measure in accordance with the law of that state. Alternatively, consideration could be given to **creating a judicial body at European level composed of authorities from all Member States and independent experts (judges and lawyers), which could be required to "greenlight" all orders going to service providers and other entities** (similar, for example, to article 15 of the Draft Legal Instrument on Government-led Surveillance and Privacy). The importance of a Judicial review mechanism to safeguard fundamental rights is already recognised in European instruments, for instance the Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO').

3. Subject matter

Article 1(1) states that the regulation concerns the cross-border acquisition and preservation of electronic *evidence* without specifying what is meant by *evidence*. In order to avoid any differences in interpretation about the subject matter of the proposed instrument, it is necessary that **Article 2** includes a clear definition of what is considered *evidence*. The definition could be formulated as follows:

- "All data which could be potentially used in court concerning a specific criminal case for the purposes of being led in evidence as to the alleged facts material to the case."

4. Scope

The CCBE considers that it is of paramount importance that production and preservation orders must conform to the requirements of necessity and proportionality. Accordingly, **EPOC's and EPOC-PR's should be issued only in connection with specific crimes and should not be issued for the purpose of monitoring alleged criminal activities.**

In Recital 29 it is stipulated that a European Production Order should only be issued if it is necessary and proportionate. The assessment should take into account whether the Order is limited to what is necessary to achieve the legitimate aim of obtaining the relevant and necessary data to serve as evidence in the "individual case only". However, in the substantive text of the proposed regulation there are no specific criteria for the necessity and proportionality test. For example, the conditions for issuing EPOC's/EPOC-PR's do not include any threshold of a sufficient degree of suspicion. **In order to avoid abuses, EPO's must be validated by the relevant authorities only if there are compelling reasons giving rise to a sufficient degree of suspicion to justify the cross-border seizure of data.**

Furthermore, **Article 3(2)** stipulates that European Production Orders and European Preservation Orders (note that in the text "Production" appears twice, with the reference to "Preservation" missing) may only be issued for "criminal proceedings", both during the pre-trial and trial phase. Also, in **Article 5(2)** it is recalled that European Production Orders must be necessary and proportionate for the purpose of the proceedings referred to in Article 3(2). However, we consider that the wording of Article 3(2) might be interpreted in a way which is inconsistent with the wording of Recital 29 which refers to the necessity for EPOC's to be issued for the purpose of an "individual case only". In view of the subject matter set out in Article 2, it is also necessary to specify that the scope of the proposal should be, and is, limited to only the cross-border acquisition and preservation of electronic *evidence*, rather than that it applies more broadly to the production and preservation of electronic data in general.

Therefore, the CCBE proposes that the wording of Article 3(2) be changed by clarifying that orders may only be issued for the purpose of obtaining evidence in the course of specific criminal proceedings. The relevant provision would then read as follows: "The European Production Orders and European Production Orders may only be issued for ***the purpose of obtaining evidence in the course of specific*** criminal proceedings, both during the pre-trial and trial phase".

5. Liability

According to Recital 46, as long as service providers act in good faith, they cannot be held liable for any damages caused because of a wrongful or unjustified execution of an EPOC or an EPOC-PR. We believe that such a broad disclaimer could be problematic in the event that, for example, privileged information is wrongfully shared with judicial authorities. Such a disclaimer might lead to a situation that service providers automatically execute requests without proper scrutiny.

Therefore, the CCBE considers that the recital needs to be more specific, especially as regards what "good faith" means.

6. Judicial validation

There appears to be no proper justification why a European Production Order (EPO) for subscriber and access data in general does not require judicial validation. It needs to be set out more clearly what type of data falls within the class of 'subscriber or access data' in order to avoid the seizure of information which would normally require independent judicial oversight in accordance with national rules, MLA procedures, or the European Investigation Order (EIO).

For example, IP addresses or interfaces fall into more than one category, i.e. access data and subscriber data (**Article 2(7)(b)**). Also, the definition of subscriber data includes not only what is usually understood under subscriber data (see Article 2(7)(a)), but also broad generic terms such as "the type of service [...] including technical data and data identifying related technical measures or interfaces [...] and data related to the validation of the use of service" (Article 2(7)(b)). These wide terms could even be taken to include data that are not related to the usual meaning of the term "type of service", such as, for example, any technical characteristics of the service provided, thus blurring the distinction between access data and subscriber data. Considering also that the new proposed e-Privacy regulation[4] uses yet another type of classification (electronic communications content and metadata), and also considering that the currently effective e-Privacy Directive[5] uses yet another definition of traffic data for roughly the same purposes, leads to a confusing situation where there are overlapping and potentially competing definitions. In these circumstances, there is a pressing need to ensure clarity and consistency of definition, limiting the number of such terms to the minimum necessary.

The fact that the recovery of subscriber and access data in general does not require judicial validation also runs counter to the recent judgement of the European Court of Human Rights (ECtHR) in the case of Benedik v. Slovenia[6] where it was held that there had been a violation of Article 8 with regard to the failure of the Slovenian police to obtain a court order before accessing subscriber information associated with a dynamic IP address. According to the Court, the legal provision used by the Slovenian police in order to access subscriber information associated with a dynamic IP address without first obtaining a court order had not met the Convention standard of being 'in accordance with the law'.

In the Tele2/Watson case[7] the CJEU held that "it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime" (par. 120). This raises the following question:

- How can validating authorities properly evaluate the appropriateness of a request to issue an EPO?
- What information will they receive other than the certificate form?
- Should this be left to each national Member State to specify or must there be some common criteria and rules?

[4] Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.
[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[6] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}
[7] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d8409b5427bcc14f3c8fb3fff95b372c57.e34KaxiLc3qMb40Rch0SaxyPaxn0?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=535293

It is important to clarify that professional secrecy/legal professional privilege can cover not only content data, but also other types of data, e.g. access data, and in such cases, judicial validation and oversight is required.

If the Regulation does not provide absolute certainty about what types of data fall into the various data categories, law enforcement authorities (LEAs) will not know whether they need judicial validation, and addressees will not be able to assess whether EPOs have been lawfully issued.

Moreover, there might be a need for the participation in the proceedings of a person who is aware of matters such as whether the evidence is likely to be covered by lawyer-client confidentiality. Normally that would be the data controller. It is appreciated that this might not always be appropriate, especially where there is a risk of destruction of the evidence.

Therefore, the CCBE suggests that EPOC's for subscriber and access data should be issued and validated by a judge, court or investigating judge and that a two-stage process could be required, the first stage being the use of a preservation order to secure the evidence before any contested application for a production order and the second stage might be the hearing (if contested) of the application for a production order.

7. Conditions for issuing a European Production Order Certificate

Requirement of double criminality

In the second part of both **Articles 3(2) and 5(2)**, it is only in relation to crimes punishable in the issuing Member State that an EPOC may be issued. **The CCBE submits that it should be made a requirement that the crime in question must be punishable in both the issuing State and the Member State where the data are sought.**

EPO's targeting subscriber data or access data

It can also be hardly justified that European Production Orders targeting subscriber data or access data can be issued for minor offences also and are not limited to serious crimes **(Article 5(3))**. This seems in conflict with the CJEU rulings in the Tele2/Watson[8] and Digital Rights Ireland case[9]. **The CCBE therefore proposes that EPO's targeting subscriber data or access data can only be issued for serious crimes.**

Conditions for EPO's targeting transactional or content data

For EPO's targeting transactional or content data, the question arises if a custodial sentence of a maximum of at least 3 years is sufficiently high to avoid that the instrument is abused to tackle small crimes. Under the penal codes of the Member States, a very large number of offences fall under this category, including offences that are not considered to constitute a serious crime. Crimes punishable of less than 3 years could also be covered if they fall within the scope of any of the referred articles of Council Framework Decision 2001/413/JHA, Directive 2011/93/EU, Directive 2013/40/EU, Directive (EU) 2017/541 (Article 5(4)). The extension of the scope to all matters with a maximum sentence of at least three years does not do justice to the severity of the interference. The CCBE is concerned that this will most likely apply to minor crimes in many Member States. **It therefore proposes to include a list of specific offenses that should be limited to serious crimes only as prescribed in the CJEU rulings.**

Addressees of European Production Orders

When responding to the public consultation on e-evidence, the CCBE stressed that when a production order is enforced, an organisation should be notified, allowed to assess its legal rights and obligations, and if possible, be able to challenge the request before any data can be seized.

This entails that requests for access to digital evidence should, whenever possible, always be addressed to the data controllers, rather than the data processors, which, especially when the data are controlled by a law firm, would provide better safeguards against any unlawful sharing of privileged information. Data processors, or other intermediaries would have no information on many important aspects of the context of the data which have been sought, and therefore would not always be in a position to assess the lawfulness of the request or any further legal requirements that would need to be fulfilled.

[8] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d8409b5427bcc14f3c8fb3fff95b372c57.e34KaxiLc3qMb40Rch0SaxyPaxn0?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=535293

[9] http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en&type=TXT&ancre=

The proposed Regulation makes clear in **Article 5(6)** that, where a European Production Order targets the data of a company or another entity other than natural person, the data should be sought in the first instance from that entity, unless doing so would undermine the investigation.

This safeguard is important since data controllers are generally in the best position to review and assert any rights that attach to the electronic evidence they are requested to hand over.

Law firms are covered by this provision and should therefore be directly addressed so that they are in a position to assess the legal requirements for fulfilling such data requests, including the fact whether the data requested are subject to professional secrecy/legal professional privilege. This exemption is therefore especially critical in cases where the requested data are held by a law firm.

The CCBE is, however, concerned about the very general wording which provides law enforcement authorities with a very wide leeway to circumvent data controllers. Furthermore, this article only applies to enterprises, whereas in most jurisdictions, sole practitioners (who make up the vast majority of European law practices) are not considered legal persons. Sole practitioner lawyers who are natural persons would thus not be subject to the same protection as law firms. Regardless of how a practice is organised (single practitioner or law firm), professional secrecy must always be protected, and all necessary safeguards require to be ensured.

Accordingly, the CCBE proposes that it is specified in Article 5(6) that the issuing authority is obliged to duly set out and justify in each case why an EPOC cannot be addressed to the data controller (i.e. company, entities other than natural persons and regulated professionals) on the basis of meaningful and documented assessments. Also, the term 'regulated professionals' should be added in the same provision.

Although Article 5(6) stipulates that where an EPO targets the data of a company or another entity other than a natural person, the data should be sought in the first instance from that enterprise, it is not clear from the substantive text in Article 5(6) nor from Recital 34 by means of what type of investigative measure the data held by such entities should be requested. In the explanatory memorandum it is indicated that "[t]his may require an EIO or MLA procedure where the company would not be a service provider covered by the scope of this Regulation". **In order to avoid any uncertainty about this, it is necessary to clarify this in the substantive text of the proposed regulation.**

European Production Orders covering privileged information must not be issued nor executed

Another key issue is that there should be exempted from the scope of the legislative instrument, data which the requesting authority knows, or ought to know, is protected by obligations of professional secrecy/legal professional privilege under the law of the issuing and/or executing State.

Article 5(7) sets out that in the event that there are reasons to believe that the requested data are covered by professional secrecy, clarification requires to be sought by contacting the relevant authorities before proceeding with the request. If the data are covered by professional secrecy obligations, the EPO must not be issued.

The question, however, arises as to how LEAs can determine who is a lawyer, especially if it is a lawyer in another Member State. Appropriate technical measures are required to ensure that both LEAs and service providers know when data are held by lawyers (and this may entail some means of verification of lawyers' identities). A pragmatic way would be to require service providers to offer lawyers an option for indicating such information – of course, only after careful verification as to whether that user is indeed a lawyer, as claimed.

In this respect, the CCBE could assist in creating a mechanism to identify lawyers on the basis of the prototype tool developed under the FAL2 project for the identification of lawyers. This tool (which is also being used in the context of the e-CODEX system) could be tailored for this specific purpose.

Furthermore, although professional secrecy/legal professional privilege is a ground to refuse judicial validation (and has to be taken into account during a criminal trial – see Article 18), it is not an explicit ground for refusal to execute an EPO. **It needs therefore to be specified in Article 9 that the fact that the requested data are covered by professional secrecy/legal professional privilege constitutes a valid ground to refuse the execution of an EPO. Also, on the form (in the Annex), an additional box should be added on professional secrecy as a reason to refuse the execution of an EPO.**

8. Conditions for issuing a European Preservation Order Certificate

Article 6(2) stipulates that a preservation order "may be issued where necessary and proportionate to prevent the removal, deletion or alteration of data in view of a subsequent request for production of this data via mutual legal assistance, a European Investigation Order or a European Production Order. European Preservation Orders to preserve data may be issued for all criminal offences." However, it lacks any safeguard against general and indiscriminate preservation of data (see cases Tele2/Watson and Digital Rights Ireland). There are also no safeguards against recurrent preservation orders which are not followed-up by production orders.

This provision must therefore be brought into line with the CJEU ruling in Tele2/Watson (see paras. 108-111). A possible solution would be to specify that EPOC-PR must concern the targeted retention of data, for the purpose of fighting serious crime, provided that the retention of data is limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned, and the retention period adopted, to what is strictly necessary.

9. Execution of a European Preservation Order Certificate

Following the wording of **Article 10**, the addressee's obligation to preserve any requested data ceases to exist after 60 days, unless it has been confirmed by the issuing authority that a subsequent European Production Order has been 'launched', though not yet 'served'. In such a situation, no time limit has been provided for the preservation of the requested data.

Accordingly, the CCBE considers that it is necessary to include a time limit for cases where the issuing authority, for whatever reason, refrains from serving the European Production Order at all.

10. Grounds for refusal to execute a European Production Order Certificate and a European Preservation Order Certificate

The CCBE considers that the grounds for refusal to execute an EPOC are too restrictive. Apart from technical or practical reasons (e.g. EPOC is incomplete or the addressee cannot comply because of *force majeur*), the only substantive ground for non-execution that may be invoked by the addressee is that if it considers that "based on the sole information contained in the EPOC it is apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive". **Therefore, there requires to be set out further specific grounds to refuse the execution of an EPO, including (as referred to above) the absence of double criminality or the fact that the requested data are covered by professional secrecy/legal professional privilege.**

As to contentious proceedings (criminal or civil litigation) *any* violation of professional secrecy/legal professional privilege is per se a violation of the right to a fair trial according to Article 6 ECHR and should as such be recognised as a sole and sufficient ground to refuse the execution of an EPO.

11. Notification to the data subject

The notification requirement set out in **Article 11(2)** can very easily be ignored by authorities since there is always a reason to find why such notification could jeopardize the investigation/proceedings. This severely undermines the rights of persons to a fair trial, because, as long as such persons are not aware that their data have been taken, they cannot assert their rights**. The CCBE considers that the imposition of confidentiality restrictions on EPOC's must be subject to the approval of an independent judicial authority and in each case be duly motivated and justified by the issuing authority on the basis of meaningful and documented assessments. With regard to European Preservation Orders, the CCBE also submits that the issuing authority must be obliged to inform the data subject.**

12. The rights of the defence

Any proposal for the recovery of electronic evidence should not be seen as solely concerned with prosecution. Rights of defence should be given proper regard. The proposal does not take properly into account the requirement for equality of arms in criminal proceedings, which is a concept recognized by the ECtHR in the

context of the right to a fair trial. Whereas prosecutors can issue production and preservation orders, no provisions exist enabling defendants or their representatives to access or request electronic evidence.

Moreover, the proposal does not provide any requirement or guidance for addressees to limit the transmission of e-evidence to data that are relevant for the purposes of the criminal proceedings. As a result, LEAs could be overwhelmed with data. There is also no provision to ensure that defendants do not in turn become over-burdened under the weight of e-evidence, or that such e-evidence will be made readily accessible by the addition of appropriate metadata such as an index and table of contents. Without the help of such metadata, it is very difficult or even impossible for lawyers effectively to assert their clients' rights.

The CCBE submits that, as with the EIO, suspected or accused persons or their lawyers should be able to request the issuing of a European Production or Preservation Orders in an equally efficient way as prosecutors can. If not, the proposal undermines the principle of equality of arms between the prosecution and defence, placing the defendant at a significant disadvantage. Moreover, addressed entities should be required to hand over only data that are relevant for the purposes of the criminal investigation.

13. Effective remedies and judicial reviews

As regards **Article 17**, the CCBE considers that **persons affected by an EPOC should not only be able to exercise their remedies before the court in the issuing state, but also in the court of the Member State where the data are sought. The CCBE considers that it is necessary also to extend the right to effective remedies in Article 17 to European Preservation Orders.**