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

29/06/2018

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. With this paper, the CCBE wishes to share its initial observations in relation to a number of aspects of the proposal. A more detailed position paper will follow in due course.

The key question arising from this legislative initiative is whether the proposal to enhance the powers to access electronic evidence across national borders by investigating authorities is coupled with sufficient procedural safeguards and due process procedures. In other words, are there any aspects that could undermine fair trial rights, and, if so, how might these aspects be addressed?

There are three core issues within which most of the detailed observations sit:

1. The provision of an effective mechanism which ensures the protection of lawyer-client communications. This raises in particular the following issues:
    a) Upon which persons should the Orders be served?
    b) How far is judicial scrutiny of applications necessary?
    c) How can the effectiveness of such scrutiny be secured?
    d) Do the proposed grounds for refusal need to be supplemented?
    e) Do the provisions for notification require to be supplemented?
2. Ensuring equality of arms between the prosecution and the defence.
3. Provision of effective judicial review

The discussion below contains certain preliminary observations on these and other matters. It is accepted that these observations are likely to be the first step in a dynamic and collaborative process in addressing the text of the Proposal in the course of the legislative process, and should be seen as a preliminary document. The CCBE will present fuller and more detailed observations as the legislative process proceeds.

1. Protection of confidentiality of lawyer-client communication

For lawyers to be effective in defending their clients' rights, there must be confidence that communications between a client and their lawyer are kept confidential. This principle – usually referred to as 'professional secrecy' or 'legal professional privilege' – is recognised by all EU countries and has been upheld by the European Court of Justice and the European Court of Human Rights in numerous cases. The violation of professional secrecy constitutes in some EU Member States not only a violation of a professional duty, but also a criminal offence.

Material which is potentially privileged will enjoy the heightened protection of article 8 of the European Convention on Human Rights (ECHR). Additionally, lawyer-client communications in relation to contentious proceedings (criminal or civil litigation) also enjoy protection under Article 6 ECHR concerning the right to a fair trial. Article 6 rights (unlike article 8 rights) are absolute in the sense that limitations or derogations cannot be applied.

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 is 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 has 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.

The proposed Regulation makes clear in **Article 5(6)** that, where a European Production Order (EPO) targets the data of an enterprise, the data should be sought in the first instance from that enterprise, 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 is subject to professional secrecy/legal professional privilege. This exemption is therefore especially critical in cases where the requested data is 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 still 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. The term 'regulated professionals' should therefore be added. Regardless of how a practice is organised (single practitioner or law firm), professional secrecy must always be protected and all safeguards have to be fulfilled to this effect,

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

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

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

The question however arises how law enforcement authorities (LEAs) can determine who is a lawyer, especially if it is a lawyer in another Member State. Some technical measures seem to be required to ensure that both LEAs and service providers know that data is held by lawyers (as well as some verification of lawyers' identity). 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 is 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.

2. Judicial validation

According to the CCBE, judicial validation by the requesting state is the minimum protection that needs to be ensured, especially given the fact that the order will no longer be cross-checked by the authority in the requested country (as is the case with mutual legal assistance (MLA) procedures).

There appears to be no proper justification why EPO's for subscriber and access data in general do not require judicial validation. It needs to be set out more clearly what type of data is considered '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 do 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 very 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 include data that is not related to the usual meaning of the term "type of service", like 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[1] uses yet another type of classification (electronic communications content and metadata), and also considering that the currently effective e-Privacy Directive[2] uses yet another definition of traffic data for roughly the same purposes, it would be very important to limit the number of such terms to the minimum necessary.

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, LEAs will not know whether they need judicial validation, and addressees will not be able to assess whether EPOs have been lawfully issued.

3. Sufficient degree of suspicion

The conditions for issuing a European Production or Preservation Order do not include any threshold of a sufficient degree of suspicion (Article 5). **In order to avoid abuses, EPO's must only be validated by the relevant authorities if there are compelling reasons giving rise to a sufficient degree of suspicion to justify the cross-border seizure of data.**

---

1 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.

2 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.

4. Effective mechanism for ensuring approval

If the rules for approval are to be effective, there is a need for the opportunity, where appropriate, for there to be 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 (in line with the above observations). It is appreciated that this might not always be appropriate, especially where there is a risk of destruction of the evidence. **In such cases, consideration should be given to having a two-stage process where a European Preservation Order might be used to secure the evidence before any contested application for a Production Order.**

5. Grounds for refusal to execute

The CCBE considers that the grounds for refusal to execute an EPO set out in **Article 9(5)** are too restrictive. Apart from technical or practical reasons (e.g. the EPO Certificate (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". **There should be more broader grounds to refuse the execution of an EPO, including the absence of double criminality or, as pointed out above, the fact that the requested data is 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.**

6. Notification of the data subject

Article 11(2) specifies that the person whose data is being sought needs to be informed "without undue delay about the data production". However, this "may be delayed as long as necessary and proportionate to avoid obstruction of the criminal proceeding". The notification requirement can therefore very easily be ignored by authorities since there is always a reason to find why it could jeopardise the investigation.

This severely undermines people's fair trial rights because as long as they are not aware that their data has been taken, they cannot assert their rights. **The imposition of confidentiality restrictions on EPOs must therefore 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.**

7. 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 recognised by the European Court of Human Rights 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.

The CCBE therefore considers 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 Order 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, the proposal does not provide any requirement or guidance for addressees to limit the transmission of e-evidence to data that is relevant for the purposes of the criminal investigation. 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 the e-evidence, or that such e-evidence will get 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 to assert effectively their clients' rights.

8. Judicial Review

Consideration should be given to the provision of an effective means of judicial review analogous to the mechanism foreseen in article 42 of the Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office, particularly in relation to the jurisdiction of the Court of Justice in accordance with Article 267 of the Treaty on the Functioning of the European Union.