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 recommendations on the establishment of international rules for cross-border access to electronic evidence

28/02/2019

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.

This paper is the CCBE's response to a number of recent developments concerning the establishment of international rules for cross-border access to electronic evidence for the purpose of criminal investigations, especially as regards so-called direct cooperation between law enforcement authorities and service providers.

A. Direct cooperation as an alternative to judicial cooperation

In view of the current fragmentation in the way cross-border access to electronic evidence is sought and processed, the CCBE in principle welcomes initiatives to create proper legal frameworks for the cross-border recovery of such evidence in a manner which provides legal certainty and greater efficiency than is the case at present. However, such initiatives should be coupled with robust safeguards for the persons whose data is accessed, including, among other safeguards, rights to protection of personal data, to an effective remedy and to a fair trial, including the presumption of innocence and a right of defence.

The CCBE does not consider that the establishment of direct cooperation mechanisms between law enforcement authorities and service providers is a satisfactory alternative to judicial cooperation between cross-border law enforcement authorities, nor is it a necessary or proportionate means to achieve the objective of greater efficiency. So-called "direct cooperation" between law enforcement authorities and service providers is not truly a mechanism for co-operation between willing parties as it is a means whereby law enforcement authorities can compel compliance by service providers, without proper judicial oversight. In particular, it undermines the essential duties of national judicial authorities to ensure that the rights of its citizens are not infringed, compromised or undermined. Such infringement arises from the circumstance that judicial authorities in the state in which the service provider is situated are, effectively, cut out of the process: they are in no position to undertake a legality check of requests for judicial cooperation emanating from the authority of another Member State. The CCBE is unable to support such measures having as their effect the curtailing of the role and responsibilities of national judicial authorities. It favours instead the approach of reviewing and improving current MLA procedures, for example by making them faster through the use of digitisation and by taking measures to better equip 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. This is especially important in relation to information communicated in confidence between lawyers and clients which is legally protected from disclosure. Also, smaller entities may lack the legal resources and expertise to query the legality of the production order. Furthermore, where the undertaking is simply a service provider, it may lack the knowledge necessary for it even to be aware that the request compromises the data subject's fundamental rights.

In these circumstances, 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. In the case of personal data within the meaning of the GDPR this would normally be the data controller (e.g. a law firm), and, in the case of data concerning a legal (as opposed to natural) person (which data would not fall within the scope of the GDPR) it would be a "controller" in an analogous position. It is appreciated that such notification might not always be appropriate, especially where there is a risk of destruction of the evidence when the data controller becomes aware that an investigation is taking place. The CCBE recognises that such situations may arise from time to time, and suggests that, in such cases, it may be acceptable to have in place an evidence preservation request process which would compel the relevant undertaking to take steps to preserve that evidence, pending the conduct of a legality check by the judicial authorities of the state in which the evidence is situated. Once the evidence has been secured through a preservation order, a proper legality check would then be undertaken prior to the production of the targeted data.

The CCBE therefore proposes that direct cooperation between law enforcement authorities in one jurisdiction and service providers in other jurisdictions be restricted to the obtaining of preservation orders alone. For the production of electronic evidence, a preservation order could be followed up with a procedure under a Mutual Legal Assistance Treaty. Apart from the reasons explained above, further arguments in favour of restricting direct cooperation to preservation orders include the procedural and technical uncertainties regarding the execution of such 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 light of the foregoing and in response to the recent Recommendations issued by the European Commission on the opening of international negotiations on cross-border rules to obtain electronic evidence, the CCBE wishes to highlight its concerns in relation to the legislative developments which are discussed below.

B. The U.S. CLOUD Act

With the adoption of the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act, US law enforcement agencies now have explicit legal authority to obtain electronic data from U.S. cloud and communication companies regardless of where the company stores the data. The CLOUD Act also proposes a legal framework for expeditious international data-sharing using executive agreements.

The CCBE joins the European Parliament in its concerns regarding the CLOUD Act, regretting that the U.S. has unilaterally sought to expand the territorial reach of its law enforcement powers, instead of making use of Mutual Legal Assistance Treaties (MLAT's)[1]. As a result, undertakings offering electronic communication and/or information society services may find themselves in the dilemma of being compelled to violate either EU legal obligations (by disclosure of personal data in compliance with a CLOUD Act warrant) or US legal obligations (by non-disclosure of personal data in compliance with EU data protection law, namely the General Data Protection Regulation).

Although the CCBE welcomes the provisions of the CLOUD Act which introduced legal remedies in respect of warrants targeting non-US citizens, it takes the view that the newly-introduced "motion to quash or modify" is too narrow in scope. Most egregiously, the bringing of a motion to quash or modify is restricted to circumstances where the laws of only a so-called "qualified government" might be violated. Furthermore, the legal process does not involve the hearing of the State in which the seized data is stored, nor is the affected person notified subsequent to the "seizure". Another major concern is that the CLOUD Act does not have any proper mechanism for the protection of the secrecy or confidentiality of evidence in the possession of lawyers, and which is subject to legal professional privilege or similar obligations of professional secrecy. For a fuller analysis and statement of the CCBE concerns in this respect reference is made to the CCBE Assessment of the U.S. CLOUD Act.

C. Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters

It is regrettable to note that the legislative initiative proposed by the European Commission as setting out a framework for direct cooperation between EU law enforcement actors and service providers to a large extent mirrors the approach taken in the U.S. CLOUD Act and, hence, gives rise to similar concerns.

Although this proposal is, of course, to be construed within a different legal context, its overall approach is broadly the same as the CLOUD Act. The main purpose of the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters is to enable law enforcement authorities of an EU Member State to oblige undertakings offering electronic communications and/or information society services in the EU to preserve and/or produce electronic evidence, irrespective of the jurisdiction in which that undertaking is based and where the data are stored.

Reference is made to the CCBE position paper[2] regarding this proposal, which gives a detailed overview of the main areas of concern. The CCBE's fundamental concern, however, is that the proposed regulation 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 position paper also sets out a number of further issues and concerns that the CCBE wishes to see addressed in the course of the legislative process, particularly in relation to the protection of confidentiality of lawyer-client communications, judicial validation, grounds for refusal of the execution of the order, the need for a sufficient degree of suspicion as justifying the granting of an order, the importance of notifying data subjects, and rights of defence.

The draft of the proposed regulation was published by the Commission in April 2018. On 7th December the Justice and Home Affairs Council approved a general approach in respect of the proposed Regulation. The approved common approach was published on 12th December. It contained a number

---

1 European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (Paragraphs 37-38).

2 CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for e evidence in criminal matters, 19 October 2018.

of significant amendments. For example, the Council common approach introduces in Article 7a a form of notification of the authorities in the Member State where the data is sought. This provision, however, does not provide any meaningful protection as the notification has no suspensive effect, there is no obligation for the Member State concerned to intervene, there are no grounds on which objections might be taken nor the request be refused, nor is there any requirement for a proportionality check.

The Council common approach also suggests deleting the grounds upon which service providers are permitted to refuse to execute production orders. It is the considered position of the CCBE that, on the contrary, not only should those grounds for refusal be preserved, but also should be widened so as to include also the absence of double criminality and the circumstance that the requested data is covered by professional secrecy/legal professional privilege.

Furthermore, the Council common approach substantially waters down the requirement to notify data subjects by stating that this may be delayed "as long as it constitutes a necessary and proportionate measure". This severely undermines the data subjects' fair trial rights because, so long as data subjects are not aware that their data has been the subject of a production request, they cannot assert their rights. As set out in the CCBE position, if data production orders (as opposed to data preservation orders) are to be permitted at all, the imposition of confidentiality restrictions on such production orders ought to 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. Also, such confidentiality restrictions should not continue any longer than is strictly necessary. When confidentiality restrictions cease, the data subjects should be informed and have available to them appropriate legal remedies.

The CCBE therefore regrets that instead of remedying the major defects which were contained in the original proposal, the Council's general approach exacerbates them and undermines even those inadequate procedural safeguards which were present in the Commission proposal.

In light of this, the CCBE welcomes what appears to be a more sceptical approach by the European Parliament to the proposal. The CCBE notes that, instead of presenting a Report, the Rapporteur for the file, Birgit Sippel MEP (S&D, Germany) first published a series of working documents which assess in detail issues such as the scope of the proposed application of the draft regulation and its relationship with other instruments; the execution of production and preservation orders and the role of service providers; the relationship of the regulation to third country laws; conditions for issuing production and preservation orders; safeguards and remedies (including data protection safeguards); and the enforcement of production and preservation orders.

These working documents will serve as the basis for the preparation of the draft Report of the LIBE Committee, which will be produced by the new Parliament following the forthcoming elections.

In this regard, it is important to note that the second working document questions the legal basis of the proposed e-evidence regulation on the ground that it goes beyond the current application of Article 82(1)(a) of the Treaty on the Functioning of the EU by appearing to seek to broaden the concept of mutual recognition as laid down therein.

The final outcome of the legislative process is therefore still highly uncertain and the CCBE considers that it is therefore premature for the European Commission to seek to negotiate international instruments using the e-evidence proposal as a reference point.

D. Second Additional Protocol to the Council of Europe Convention on Cybercrime

Similar developments are also taking place within the context of the Second Additional Protocol to the Council of Europe Convention on Cybercrime ('Budapest Convention', CETS No. 185) which is currently

being negotiated. In accordance with the Terms of Reference, the Second Additional Protocol may include the following elements:

- Provisions for more effective mutual legal assistance, in particular:
    - a simplified regime for mutual legal assistance requests for subscriber information;
    - international production orders;
    - direct cooperation between judicial authorities in mutual legal assistance requests;
    - joint investigations and joint investigation teams;
    - requests in the English language;
    - audio/video hearing of witnesses, victims and experts;
    - emergency Mutual Legal Assistance (MLA) procedures.
- Provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests;
- Clearer framework and stronger safeguards for existing practices of transborder access to data;
- Safeguards, including data protection requirements.

From what has been reported so far on the current state of play of the ongoing negotiations, a similar approach is being envisaged as the U.S. CLOUD Act and the EU proposal on e-evidence. The abovementioned CCBE concerns will therefore also apply in this context.

E. CCBE Recommendations

The creation of mechanisms which no longer require an MLAT to enable law enforcement authorities to compel international data transfers has, as a consequence, the removal of the checks and balances that are built into MLATs regarding the exchange of data between the EU and the U.S. or the countries who are parties to the Budapest Convention.

In the context of the negotiation of the proposed EU-U.S agreement as well also as the negotiations concerning a Second Additional Protocol to the Council of Europe Convention on Cybercrime, the CCBE therefore strongly calls upon the EU institutions to adhere to the following principles so as to prevent any potential conflicts with European law, to create sufficient safeguards and legal remedies against third country surveillance measures and to ensure the protection of legal professional privilege and professional secrecy:

1. To postpone the negotiation of the proposed EU-U.S. agreement and the Second Additional Protocol to the Council of Europe Convention on Cybercrime until the legislative process concerning the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters is finalised.
2. To ensure respect for the fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties, the EU Charter of Fundamental Rights and the European Convention on Human Rights.
3. To restrict direct cooperation with service providers in other jurisdictions so as to relate to preservation orders only, though admitting of the possibility that, a preservation order relating to electronic evidence, might be followed up with an appropriate procedure under a Mutual Legal Assistance Treaty to recover that evidence.

In the event that the European Institutions were to decide to proceed with establishing direct cooperation instruments for international production orders concerning electronic evidence, the CCBE

urges them to take into account the following minimum requirements that should be met by such instruments, namely, that they should:

1. Establish a general prior judicial review mechanism including a framework for the protection of legal professional privilege and professional secrecy.
2. Ensure that following a production order, data will be transferred to the requesting (third) country only after notification had been given to a competent and independent EU Member State authority.
3. Ensure that the addressed service provider which is processing the requested data is informed by the competent EU Member State authority about existing legal remedies.
4. Ensure sufficient safeguards and grounds for refusal to execute international production orders, including the absence of double criminality or the fact that the requested data are covered by professional secrecy/legal professional privilege. The latter should be stated explicitly and constitute an absolute ground for refusal to execute an order.
5. Ensure that the imposition of confidentiality restrictions on production orders 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.
6. Ensure that confidentiality restrictions do not continue any longer than is strictly necessary. When confidentiality restrictions cease, the data subjects should be informed and have available to them appropriate legal remedies.
7. Ensure that suspected or accused persons, or their lawyers are able to request the issuing of international production or preservation orders in an equally efficient way as is possible for law enforcement authorities, so as to ensure the observance of the principle of equality of arms between the prosecution and defence, without which the defendant is placed at a significant disadvantage.