EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of European Lawyers
Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

CCBE comments

Draft 2nd Additional Protocol to the Convention on Cybercrime

Provisional draft text of provisions (1 October 2019) on Language of requests, Emergency MLA, Video Conferencing, direct disclosure of subscriber information, and giving effect to orders from another Party for expedited production of data

8 November 2019

Introduction

*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.*

With this paper the CCBE submits its written comments in response to the public consultation regarding the provisional draft text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime.

The CCBE has followed with great interest the latest activities of the Cybercrime Convention Committee, particularly as regards access to electronic evidence.

As you may understand, lawyers play a fundamental role – not only towards their clients, but also vis-à-vis law enforcement authorities – when it comes to the cross-border acquisition and exchange of electronic evidence in criminal matters.

The CCBE has therefore issued a number of position papers on this matter, such as:

- CCBE recommendations on the establishment of international rules for cross border access to e-evidence (FR)
- CCBE position on Commission proposal Regulation on European Production and Preservation Orders for e evidence in criminal matters (FR)

In addition, the recently published CCBE Recommendations on the protection of fundamental rights in the context of "national security" (FR) are also highly relevant in this context.

Please find below a number of suggestions and observations in relation to the Provisional draft text of the provisions which were published on 1 October 2019, particularly as regards Video Conferencing and Direct Disclosure of Subscriber Information.

Provisions on Videoconferencing

The provisions under **Section 2** authorise the use of videoconferencing ("VC") technology to take testimonies or statements.

The CCBE's main observation in this respect is the total lack of any binding requirements or minimum procedural safeguards which requesting and requested Parties need to adhere to when conducting hearings in which video-link is used. Especially in relation to the hearing of a suspect or accused person

(**Section 2.1, paragraph 7**), it is striking that the draft provision leaves it to the complete discretion of the requested Party to require particular conditions and safeguards with respect to the taking of testimony or a statement from such person.

It is broadly recognised that some of the fundamental rights and principles of criminal procedure enshrined in the European Convention of Human Rights (ECHR) and the Charter of Fundamental Rights of the EU (EU Charter) could potentially be compromised during a hearing by VC in a cross-border case.[1]

In particular, the right to a "fair" hearing enshrined in Art. 6(1) ECHR, and the rights of the suspected and accused persons to defend themselves in person, through legal assistance of his/her own choosing or to be given it free (Art. 6(3)(c)), the right to examine witnesses against him/her (Art. (3)(d)), and the right to have the free assistance of an interpreter (Art. 6(3)(d)), may be affected.

The Council of Europe should be particularly vigilant in ensuring that these principles are not undermined through its own conventions. Also, the Council of the European Union should be called upon to adhere to its own recommendations on the use of VC which are available on the European e-Justice Portal.[2]

Although the use of VC technology may bring a number of advantages, judicial authorities must look beyond convenience alone to determine whether in the circumstances of the individual case, the use of VC is, on balance, beneficial to the overall fair and efficient administration of justice.[3]

In cross-border cases, particularly where the parties might not be native speakers and will be subject to different cultural influences, the investigative judge or prosecutor might not be able to examine so easily the nuances of the parties' appearances and responses through a video-link. Moreover, judicial authorities might have a tendency to ask fewer questions and be less likely to interrupt an argument, which might not be a beneficial outcome for the parties.

Therefore, **it is important that the Council of Europe develops mandatory minimum standards as to the technical arrangements that should be in place for the use of videoconferencing to ensure as much as possible a true-to-life hearing experience including full communication/interaction of all the parties to the procedure with the examined person**. Technical arrangements must also ensure that the VC is protected from **improper access (hacking)**. Consumer-level videoconferencing services, such as Skype or FaceTime, are inadequate in this respect. Such mandatory minimum standards should also ensure **protection of professional secrecy and legal professional privilege** during the VC session.

Furthermore, the **possibility for lawyers to participate in a hearing conducted through video-link** in order to defend their clients' interests must also be explicitly mentioned. In this regard, the CCBE recommends the following:

a) In some countries the use of VC might be subject to the participants' approval. **It therefore needs to be verified whether it is necessary to seek explicit consent of them to participate in a VC, and, if so, under what conditions participants can refuse a VC, and whether a lawyer needs to be present/consulted if participants explicitly consent or refuse.**

b) During a VC session, **the lawyer(s) (in all jurisdictions participating in the VC) should be able to sit together with his/her/their client(s)**. If this is not possible, arrangements must be made in order to enable the lawyer(s) to participate in the VC from another location.

---

1 See, e.g., Council of the European Union, "D1a: Judicial use cases with high benefits from cross-border videoconferencing", Multi-aspect initiative to improve cross-border videoconferencing ("Handshake" Project), 2017, pp. 2, 26-27, available here: https://e-justice.europa.eu/fileDownload.do?id=c87e10f3-95d9-402a-89b8-fc5c663106a6; R. A. Williams, "Videoconferencing: Not a foreign language to international courts", Oklahoma Journal of Law and Technology, vol. 7 (54), 2011, p. 21 .

2 https://e-justice.europa.eu/content_general_information-69-en.do.

3 Draft Guide to Good Practice on the Use of Video-Link under the Evidence Convention of the Hague Conference on Private International Law, available here: https://assets.hcch.net/docs/e0bee1ac-7aab-4277-ad03-343a7a23b4d7.pdf.

c) The requesting and requested court/judicial authority must **ensure that the lawyer is able to confer confidentially with her/his client** (both in case lawyer and client are sitting together or remotely from each other);

d) The court/judicial authority needs to **notify the parties, including their lawyers, of the date, time (taking into account different time zones), place and the conditions for participation in the VC**. Sufficient advance notice should be given.

e) The requesting and requested court **ensure that lawyers are able – if necessary – to identify themselves** in accordance with national rules towards the (cross-border) judicial authorities.

f) **Instructions need to be provided to the lawyer by the relevant court/judicial authority as to the procedure they need to follow to present documents or other material during the VC**. Arrangements need to be made to ensure that all participants in the VC can see the material that is presented during the VC.

g) The procedure should allow that **the participant testifies in presence of judicial authorities** who will ensure that he/she is not instructed by other participants. It should be guaranteed that the participant to be heard does not confer with any person during her/his testimony as this may have an adverse impact on the proceedings.

h) In cases where documents must be shown to a witness, that should be done via an independent person present with them (court clerk or similar) who can ensure (e.g. from the point of view of the prosecutor) that they are looking at the right page and (from the defendant's point of view) also ensure they are not looking at other documents, especially not to documents that have not been disclosed to the defendant or other parties.

The essence of these aspects needs to be reflected in both the substantive provisions under **Section 2.1** and the explanatory text.

Provisions on Direct Disclosure of Subscriber Information

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 Party. 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 Party in which the service provider is situated, there is a risk that the service provider 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 concerning lawyer-client communications 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 production orders 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 production orders?

In the event that the Council of Europe Cybercrime Convention Committee were to decide to proceed with establishing a direct cooperation instrument for international production orders concerning subscriber information, the CCBE urges to take into account the following minimum requirements, namely, that it should:

1. Establish a general **prior judicial review mechanism** including a framework for the **protection of legal professional privilege and professional secrecy**. Under **Section 4.1 paragraph 2.a** it is left

to the complete discretion of the Convention Parties to require that orders for the production of subscriber information "must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision." When the Convention Parties do not make such a declaration, service providers would be required to respond to production orders from cross-border police authorities without any form of judicial supervision. The fact that the recovery of subscriber information in general does not require judicial validation runs counter to the recent judgement of the European Court of Human Rights (ECtHR) in the case of Benedik v. Slovenia[4] 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'.

2. Ensure that following a production order**, data will be transferred to the requesting country only after notification has been given to a competent and independent Party authority**. In **Section 4.1 paragraph 5.a** it is left to the complete discretion of the Convention Parties to require the issuing Party to simultaneously notify it of any order sent directly to a service provider in its territory either in every instance or in identified circumstances. In the same way, it is not obligatory for Convention Parties to require service providers to consult the Party's authorities in identified circumstances prior to disclosure (**Section 4.1 paragraph 5.b)**.

3. **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 in **Section 4.1 paragraph 5.a and 5.b** and constitute an absolute ground for refusal to execute an order. The CCBE wishes to stress that professional secrecy/legal professional privilege can cover not only content data, but also other types of data (e.g. traffic data and, in certain circumstances, subscriber information). Furthermore, it is necessary to be sensitive to the circumstance that where recovery of subscriber data are sought, that is often the precursor to other investigative activities. Where the data relate to lawyers, recovery of it will bring a substantial risk of subsequent violation of the legal professional privilege attaching to their communications with their clients, and even where the subscriber data relate to non-lawyers, there may be a risk that subsequent investigation will lead to an infringement of privileged communications. To guard against these dangers, judicial validation and oversight is required. Moreover, 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 a production order. At this moment, the draft provisions do not offer any refusal grounds for service providers.

4. Ensure that the addressed service provider which is processing the requested data is informed by the competent Party authority about existing legal remedies, such as the grounds for refusal.

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.**

[4] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}

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.
8. **Ensure that production orders targeting subscriber information can only be issued for serious crimes**. It can hardly be justified that orders targeting subscriber information can be issued for minor offences also and are not limited to serious crimes. This seems in conflict with the CJEU rulings in the Tele2/Watson[5] Tele2/Watson and Digital Rights Ireland case[6].

[5] 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

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