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 on the Draft 2nd Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (version 12 April 2021)

30/04/2021

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.

Introduction

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 position on Commission proposal Regulation on European Production and Preservation Orders for e evidence in criminal matters** (19/10/2018)[1]
- **CCBE Recommendations on the protection of fundamental rights in the context of "national security"** (29/03/2019)[2].

In particular, the CCBE has adopted specific comments and recommendations as regard to the drafting of a 2nd Addition Protocol to the Convention on Cybercrime.

- **CCBE recommendations on the establishment of international rules for cross border access to e-evidence** (28/02/2019)[3];
- **CCBE written comments on the draft 2nd Additional Protocol to the Convention on Cybercrime** (8 November 2019)[4].

[1] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20181019_CCBE-position-on-Commission-proposal-Regulation-on-European-Production-and-Preservation-Orders-for-e-evidence.pdf

[2] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf

[3] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20190228_CCBE-recommendations-on-the-establishment-of-international-rules-for-cross-border-access-to-e-evidence.pdf

[4] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20191108_CCBE-written-comments-on-Draft-2nd-Additional-Protocol-to-the-Convention-on-Cybercrime.pdf

Please find below a number of suggestions and observations in relation to the Provisional draft text of the provisions from 12 April 2021.

A. General comments

The CCBE notes that its recommendations and comments regarding the 2nd draft additional Protocol, from 2019, were not taken into consideration in the new 2021 version of the draft**. Therefore, the CCBE reiterates the concerns raised in 2019 and calls for these to be addressed in the last version of the draft**.

Regarding the establishment of direct cooperation instruments for international production orders concerning electronic evidence, the CCBE urges for the adoption of the following **minimum requirements** that should be met by such instruments:

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 Member State authority.**

3. **Ensure that the addressed service provider which is processing the requested data is informed by the competent 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[5].**

B. Disclosure of subscriber information

Article 7 of the new version of the draft 2nd additional Protocol, "***Disclosure of subscriber information***", provides for a direct cooperation mechanism between law enforcement authorities in one jurisdiction and service providers in other jurisdictions. **Article 8** provides for a procedure "***Giving effect to orders from another party for expedited production of subscriber information and traffic data***".

[5] CCBE recommendations on the establishment of international rules for cross border access to e-evidence, 28/02/2019, p.6

As above mentioned, the CCBE notes that its comments from November 2019 were not taken into account and that only minor changes have been made in the draft regarding discloser of subscriber information. **The CCBE recalls that 2019 comments are still valid and constitute minimum requirements for ensuring respect of fundamental rights**.

- **Status of the requesting authority**

The CCBE notes that according to article to **Art. 7(2)(b)**, it is at the discretion of the Party to provide that an order "*must be issues by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision*". However, as notices by the European Data Protection Board ("EDPB"), such provision could be interpreted as allowing any "authority" to issue an international order for the discloser of subscriber information, in contradiction with EU Law and ECHR Law[6].

In its contribution, the EDPB considered that the type of requesting authority who may issue such order should be limited to **prosecutor, a judicial authority or another independent authority**.

Furthermore, the CCBE considers that the issuing of an order to disclose subscriber information should also be requested on behalf of a suspected or accused person, within the framework of applicable defence rights in accordance with national criminal procedures. According to the CCBE, suspected or accused persons or their lawyers should be able to request the issuing of an international order in an equally efficient way as prosecutors or judicial authorities can. If not, the Protocol would undermine the principle of equality of arms between the prosecution and defence, placing the defendant at a significant disadvantage.

- **Mandatory involvement of the executing authority**

The CCBE stresses that it should be mandatory for the executing authority to give its explicit approval before an international order can be executed. This guarantees that executing authorities assess and take a decision about requests, that all orders are verified against the judicial principles of *ne bis in idem* and dual criminality and that all fundamental rights and special protections are respected. In this regard, the CCBE observes that **Article 7(5)** provides that a Party may require that an order issued to a service provider in its territory is simultaneously notified to its authorities and that the designated authority may instruct the service provider no to disclose the information if conditions or grounds for refusal would apply under Articles 25.4 and 27.4 of the Budapest Convention. However, this provision only creates a possibility which remain at the discretion of each Party at the Convention. Also, article **7(5)** does not mention what kind of authority of the requested Party is to be notified.

Further, the CCBE considers that a Court authorisation in the executing Party shall be required. The aim to preserve and transmit electronic evidence in a swift manner by directly addressing the service providers must not disregard the fact that service providers are no judicial authorities that can assess the legality of an order. As recalled by the European Data Protection Supervisor ("EDPS"), "*conditions for issuing an order are not harmonised on substance at international level ant important objections against the recognition and enforcement of such order may exist. Furthermore, private entities may not be equipped to effectively deliver the required assessment. It is critical to keep in mind that despite being addressees of orders, service providers are not the one whose rights to privacy and to personal data protection are limited by the order*"[7]. It is therefore crucial to provide for judicial control in the executing State.

[6] EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), Brussels, 13 November 2019, page 4

[7] EDPS Opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention

Regarding the Court authorisation, the CCBE notes that the procedure laid down in Article 8 provides that each Party shall empower its competent authorities to issue an order compelling a service provider in its territory to produce data on behalf of another Party; to give effect to an order from another Party. However, this provision only mentions a "Competent authority" whereas it should mention a **independent judicial authority**.

- **Requirements to issue an international order and privileges and immunities**

The CCBE considers that in addition to providing for appropriate safeguards for fundamental rights, the protocol should also ensure the respect of other safeguards attached to the data such **as privilege and immunities**. Reference should be made to the immunities and privileges granted by, not only the law of the State of the service provider, but also by the law of the State where the person whose data is sought resides or is bound by an obligation of professional secrecy or lawyer-client privilege.

One problem in relation to any access to lawyers' data stored online, is the existing difficulty of identifying in advance whether data are covered by professional secrecy, legal professional privilege ("PS/LPP"). The CCBE acknowledges that Internet service providers have not yet the means, or, if they do so, then only on a very limited basis, to recognise whether the data requested by law enforcement authorities is covered by professional secrecy[8]; it is, therefore, possible that access may be given to protected data, leading to breaches of PS/LPP. **In this regard, the CCBE stresses that that Internet service providers and the Parties should be required to ensure that the technology used to collect, process and exchange personal data amongst them guarantees that there is no interference with any kind of data protected by professional secrecy**.

- **Grounds for non-recognition or non-execution of an international order**

Concerning the grounds to refuse the execution, the draft Protocol, in its article **7(5)**, only mentions Article 25.4 (national law of the requested party or MLAT) and 27.4 (political offence; interference with sovereignty, security, public order, other essential interests) of the Budapest Convention. **Further specific grounds are needed, including the absence of double criminality and the fact that the requested data are covered by PS/LPP, which should be an absolute ground for refusal to execute and order, explicitly mentioned in the Protocol.**

- **Notification requirements and confidentiality restrictions**

Concerning notification to the data subject, the CCBE recalls that confidentiality restrictions should be subject to the approval of an independent judicial authority, be duly motivated and justified by the issuing authority based on meaningful and documented assessments. The CCBE notes and welcomes the provisions of Article 14 concerning the protection of personal data.

- **Effective remedies and judicial review**

The CCBE stresses that individuals affected by an international order 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. As recalled by the EDPB and the EDPS, it is of paramount importance that the additional protocol includes mechanism to ensure the availability of legal remedies to the data subject whose data has been obtained, at least equivalent to those available in a domestic case.

[8] Talks conducted between the CCBE and EURO-ISPA (European association of European Internet Services Providers Associations, https://www.euroispa.org/about/).

C. Videoconferencing

The CCBE recalls that 2019 comments are still valid and constitute minimum requirements for ensuring respect of fundamental rights. Regarding the new Article 11 on videoconferencing of the draft addition protocol, the CCBE refers to the 2019 comments in Annex 1. In particular, the CCBE stresses that the **possibility for lawyers to participate in a hearing conducted through video-link** in order to defend their clients' interests must be explicitly mentioned.

ANNEXES

ANNEXE 1

CCBE written comments on the draft 2nd Additional Protocol to the Convention on Cybercrime (8 November 2019)

ANNEXE 2

CCBE recommendations on the establishment of international rules for cross border access to e-evidence (28 February 2019)

ANNEXE 1

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 visà-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.[9]

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 eJustice Portal.[10]

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.[11]

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.

[9] 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 .

[10] https://e-justice.europa.eu/content_general_information-69-en.do.

[11] 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.

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.

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[12] 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

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

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.**

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[13] Tele2/Watson and Digital Rights Ireland case[14].

[13] 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

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

ANNEXE 2

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)[15]. 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.

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

Reference is made to the CCBE position paper[16] 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 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

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

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.