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

Comentarios de CCBE

Proyecto del Segundo Protocolo Adicional del Convenio sobre la Ciberdelincuencia

Proyecto de texto provisional de las disposiciones (1 de octubre de 2019) sobre el idioma de las solicitudes, el eje de acción de emergencia, las videoconferencias, la divulgación directa de la información del suscriptor y la ejecución de las órdenes de otra Parte para la producción acelerada de datos.

8 de noviembre de 2019

Introducción

El Consejo de la Abogacía Europea *(CCBE) representa a las Abogacías de 45 países, y a través de ellos a más de 1 millón de abogados europeos.*

Con este documento, CCBE presenta sus comentarios por escrito en respuesta a la consulta pública sobre el proyecto de texto provisional del Segundo Protocolo Adicional del Convenio de Budapest sobre la Ciberdelincuencia.

CCBE ha seguido con gran interés las últimas actividades del Comité del Convenio sobre la Ciberdelincuencia, en particular en lo que respecta al acceso a las pruebas electrónicas.

Como comprenderá, los abogados desempeñan un papel fundamental -no sólo con respecto a sus clientes, sino también con respecto a las autoridades encargadas de hacer cumplir la ley- cuando se trata de la adquisición e intercambio transfronterizo de pruebas electrónicas en asuntos penales.

Por ello, CCBE ha publicado una serie de documentos de posición sobre esta cuestión, como por ejemplo:

- Recomendaciones de CCBE sobre el establecimiento de normas internacionales para el acceso transfronterizo a las pruebas electrónicas (FR)
- Posición de CCBE sobre la propuesta de la Comisión de Reglamento relativo a las órdenes europeas de presentación y conservación de pruebas electrónicas en materia penal (FR)

Además, las Recomendaciones CCBE sobre la protección de los derechos fundamentales en el contexto de la "seguridad nacional" (FR), recientemente publicadas, son también muy relevantes en este contexto.

A continuación se presentan algunas sugerencias y observaciones en relación con el Proyecto de texto provisional de las disposiciones que se publicaron el 1 de octubre de 2019, en particular en lo que se refiere a las videoconferencias y a la Divulgación Directa de la Información del Suscriptor.

Disposiciones sobre la videoconferencia

Las disposiciones de la **Sección 2** autorizan el uso de la tecnología de videoconferencia ("VC") para tomar testimonios o declaraciones.

La principal observación de CCBE a este respecto es la ausencia total de requisitos vinculantes o de garantías procesales mínimas de que las partes, requirente y requerida, deben respetar al celebrar audiencias en las que se utilice el enlace del vídeo. Especialmente en relación con la audiencia de un sospechoso o acusado **(Sección 2.1, párrafo 7),** es sorprendente que el proyecto de disposición deje a la entera discreción de la parte requerida exigir condiciones y salvaguardias particulares con respecto a la toma de testimonio o a la declaración de dicha persona.

Se reconoce ampliamente que, algunos de los derechos fundamentales y principios del procedimiento penal consagrados en el Convenio Europeo de Derechos Humanos (CEDH) y en la Carta de los Derechos Fundamentales de la UE (Carta de la UE), podrían verse comprometidos durante una audiencia de la VC en un caso transfronterizo.[1]

En particular, el derecho a un juicio "justo" consagrado en el artículo 6(1) CEDH y los derechos de los sospechosos y acusados a defenderse personalmente, mediante la asistencia jurídica de su elección o a recibirla gratuitamente (art. 6(3)(c)), el derecho a interrogar a los testigos en su contra (art. 3) (d) y el derecho a la asistencia gratuita de un intérprete (art. 6(3)(d)) pueden verse afectados.

El Consejo de Europa debería estar especialmente atento para garantizar que estos principios no se vean socavados por sus propios convenios. Asimismo, debería pedirse al Consejo de la Unión Europea que se adhiera a sus propias recomendaciones sobre el uso de la VC, que están disponibles en el Portal de Justicia en Red Europea.[2]

Aunque el uso de la tecnología de la VC puede aportar una serie de ventajas, las autoridades judiciales deben mirar más allá de la conveniencia por sí solas para determinar si, según las circunstancias del caso individual, el uso de la VC es, en general, beneficioso para una administración de justicia justa y eficiente[3].

En los casos transfronterizos, en particular cuando las partes no son hablantes nativos y están sujetas a diferentes influencias culturales, es posible que el juez de instrucción o el fiscal no puedan examinar con tanta facilidad los matices de las comparecencias y respuestas de las partes a través de un enlace de vídeo. Además, las autoridades judiciales podrían tender a hacer menos preguntas y tener menos probabilidades de interrumpir un argumento, lo que podría no ser un resultado beneficioso para las partes.

Por lo tanto, **es importante que el Consejo de Europa elabore unas normas mínimas obligatorias en cuanto a las disposiciones técnicas para el uso de la videoconferencia, a fin de garantizar en la medida de lo posible una experiencia auditiva real, incluida una comunicación o interacción plena de todas las partes en el procedimiento con la persona examinada**. Las medidas técnicas también deben garantizar que la VC esté protegida contra el **acceso indebido (hacking)**. Los servicios de videoconferencia a nivel del consumidor, como Skype o FaceTime, son inadecuados a este respecto. Estas normas mínimas obligatorias deberían garantizar también la **protección del secreto profesional y del privilegio profesional legal** durante la sesión de la VC.

Además, también debe mencionarse explícitamente la **posibilidad de que los abogados participen en una audiencia a través de un enlace de vídeo** para defender los intereses de sus clientes. En este sentido, CCBE recomienda lo siguiente:

---

[1] Véase, por ejemplo, Consejo de la Unión Europea, "D1a: Judicial use cases with high benefits from cross-border videoconferencing", Multi-aspect initiative to improve cross-border videoconference (Proyecto "Handshake"), 2017, pp. 2, 26-27, disponible aquí C:\Users\Stagiaire\Downloads\Handshake-project-outcomes_EU_EU_en.zip; 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] Proyecto de guía de buenas prácticas sobre el uso de enlaces de vídeo en el marco del Convenio sobre Pruebas de la Conferencia de La Haya de Derecho Internacional Privado, disponible en: https://assets.hcch.net/docs/e0bee1ac-7aab-4277-ad03-343a7a23b4d7.pdf

a) En algunos países, el uso de la VC podría estar sujeto a la aprobación de los participantes. **Por lo tanto, es necesario verificar si es necesario obtener su consentimiento explícito para participar en una VC y, en caso afirmativo, en qué condiciones los participantes pueden rechazar una VC, y si es necesario que un abogado esté presente o sea consultado si los participantes consienten o se niegan explícitamente.**

b) Durante una sesión de VC, **los abogados (en todas las jurisdicciones que participan en la VC) deben poder sentarse junto con su(s) cliente(s)**. Si esto no es posible, se deben hacer arreglos para que los abogados puedan participar en la VC desde otro lugar.

c) El tribunal o autoridad judicial requirente y la autoridad judicial requerida deben **garantizar que el abogado pueda hablar confidencialmente con su cliente** (tanto en el caso de que el abogado como el cliente estén sentados juntos o separados);

d) El tribunal o autoridad judicial debe **notificar a las partes, incluidos sus abogados, sobre la fecha, la hora (teniendo en cuenta los diferentes husos horarios), el lugar y las condiciones de participación en la VC**. Debe notificarse con suficiente antelación.

e) El órgano jurisdiccional requirente y el órgano jurisdiccional requerido **velarán por que los abogados puedan, en caso necesario, identificarse** de conformidad con las normas nacionales ante las autoridades judiciales (transfronterizas).

f) **El tribunal o autoridad judicial competente debe dar instrucciones al abogado sobre el procedimiento que debe seguir para presentar documentos u otro material durante la VC**. Es necesario hacer arreglos para asegurar que todos los participantes en la VC puedan ver el material que se presenta durante la VC.

g) El procedimiento debe permitir que **el participante testifique en presencia de autoridades judiciales** que se asegurarán de que no sea instruido por otros participantes. Debe garantizarse que el participante que va a ser escuchado no consulte con ninguna persona durante su testimonio, ya que esto puede tener un impacto adverso en los procedimientos.

h) En los casos en que los documentos deban mostrarse a un testigo tendrá que hacerse a través de una persona independiente que esté presente con él (secretario judicial o similar) y que pueda asegurarse (por ejemplo, desde el punto de vista del fiscal) de que está mirando la página correcta y (desde el punto de vista del acusado) de que no está mirando otros documentos, especialmente aquellos que no han sido revelados al acusado o a otras partes.

La esencia de estos aspectos debe reflejarse tanto en las disposiciones sustantivas de la **Sección 2.1** como en el texto explicativo.

Disposiciones sobre la divulgación directa de la información del suscriptor

En vista de la actual fragmentación sobre la forma en la que se busca y procesa el acceso transfronterizo a la prueba electrónica, CCBE, en principio, acoge con satisfacción las iniciativas encaminadas a crear marcos jurídicos adecuados para la recuperación transfronteriza de dichas pruebas de manera que ofrezcan una mayor seguridad jurídica y una mayor eficiencia que en la

actualidad. Sin embargo, estas iniciativas deben ir acompañadas de sólidas salvaguardias para las personas a cuyos datos se accede, entre las que se incluyen, entre otras, el derecho a la protección de los datos personales, a un recurso efectivo y a un juicio justo, incluida la presunción de inocencia y el derecho a la defensa.

CCBE no considera que el establecimiento de mecanismos de cooperación directa entre las autoridades policiales y los proveedores de servicios sea una alternativa satisfactoria a la cooperación judicial entre las autoridades policiales y aduaneras transfronterizas, ni que sea un medio necesario o proporcionado para lograr el objetivo de una mayor eficiencia. La denominada "cooperación directa" entre las autoridades policiales y los prestadores de servicios no es en sí un mecanismo de cooperación entre partes dispuestas, ya que es un medio por el que las autoridades policiales pueden obligar a los prestadores de servicios a cumplir sus obligaciones sin una supervisión judicial adecuada.

En particular, socava los deberes esenciales de las autoridades judiciales nacionales de garantizar que los derechos de sus ciudadanos no se vean vulnerados, comprometidos o socavados. Esta infracción se deriva de la circunstancia de que las autoridades judiciales del Estado en el que está situado el prestador de servicios están, de hecho, excluidas del proceso: no están en condiciones de llevar a cabo un control de legalidad de las solicitudes de cooperación judicial que emanan de la autoridad de otra Parte. CCBE no puede apoyar estas medidas que tienen como efecto reducir el papel y las responsabilidades de las autoridades judiciales nacionales.

Favorece, en cambio, el enfoque de revisar y mejorar los actuales procedimientos MLA, por ejemplo, haciéndolos más rápidos mediante el uso de la digitalización y tomando medidas para equipar mejor a las autoridades nacionales a fin de que puedan responder a las solicitudes transfronterizas.

Sin algún tipo de control de legalidad por parte de las autoridades judiciales competentes de la Parte en la que está situado el prestador de servicios, existe el riesgo de que se le exija al prestador de servicios que revele información de una naturaleza que normalmente no podría exigirse en la jurisdicción en la que se solicitan los datos. Esto es especialmente importante en relación con la información relativa a las comunicaciones abogado-cliente, que está protegida legalmente contra su divulgación. Además, las entidades más pequeñas pueden carecer de los recursos legales y la experiencia para cuestionar la legalidad de la orden de presentación. Además, cuando la empresa es simplemente un prestador de servicios, puede carecer de los conocimientos necesarios para saber incluso que la solicitud compromete los derechos fundamentales del interesado.

En estas circunstancias, además de la necesidad de un control de legalidad de la orden de presentación por parte de las autoridades judiciales competentes del país en el que se solicitan los datos, también podría ser necesaria la participación en las actuaciones de una persona o entidad que tenga conocimiento sobre la confidencialidad abogado-cliente. En el caso de los datos personales en el sentido del GDPR, normalmente se trataría del responsable del tratamiento (por ejemplo, un bufete de abogados) y, en el caso de los datos relativos a una persona jurídica (y no a una persona física) (cuyos datos no estarían incluidos en el ámbito del GDPR), se trataría de un "responsable del tratamiento" en una posición análoga. Es de agradecer que dicha notificación no siempre sea apropiada, especialmente cuando exista el riesgo de destrucción de las pruebas cuando el responsable del tratamiento tenga conocimiento de que se está llevando a cabo una investigación. CCBE reconoce que estas situaciones pueden surgir de vez en cuando y sugiere que, en tales casos, puede ser aceptable establecer un proceso de solicitud de preservación de pruebas que obligue a la empresa pertinente a tomar medidas para preservar dichas pruebas, a la espera de que las autoridades judiciales del Estado en el que se encuentran las pruebas lleven a cabo un control de legalidad. Una vez que las pruebas han sido obtenidas mediante una orden de preservación, se llevará a cabo un control de legalidad adecuado antes de la producción de los datos objetivo.

Por consiguiente, CCBE propone que la cooperación directa entre las autoridades encargadas de hacer cumplir la ley de una jurisdicción y los proveedores de servicios de otras jurisdicciones se limite únicamente a la obtención de órdenes de preservación. Para la presentación de pruebas electrónicas, una orden de preservación podría ir seguida de un procedimiento en el marco de un Tratado de Asistencia Judicial Recíproca. Aparte de las razones explicadas anteriormente, otros argumentos a favor de restringir la cooperación directa a las órdenes de preservación incluyen las incertidumbres técnicas y de procedimiento relativas a la ejecución de tales órdenes de presentación dirigidas a entidades privadas en otra jurisdicción sin la participación de las autoridades en las que se solicitan los datos, incluyendo:

- ¿Cómo deben servirse los pedidos de producción a los destinatarios (por correo certificado, por vía electrónica, por un sistema de entrega especial, etc.)?
- ¿Cómo se espera que los destinatarios presenten los datos solicitados a la autoridad emisora (medios, formatos, estructura, límites de tamaño, etc.)?
- ¿Cómo se puede garantizar la seguridad de la transacción para asegurar que los datos sean verdaderos, exactos y sin alteraciones?
- ¿Cómo pueden los destinatarios evaluar la autenticidad y legalidad de las órdenes de presentación?

En el caso de que el Comité del Convenio sobre la Ciberdelincuencia del Consejo de Europa decidiera establecer un instrumento de cooperación directa para las órdenes de producción internacionales relativas a la información de los abonados, CCBE insta a que se tengan en cuenta los siguientes requisitos mínimos, a saber, que debería hacerlo:

1. Establecer un mecanismo general de revisión judicial previa que incluya un marco para la **protección del secreto profesional**. Bajo la **Sección 4.1 párrafo 2.a** se deja a la entera discreción de las Partes en el Convenio para exigir que las órdenes de presentación de información sobre los suscriptores "sean emitidas por un fiscal u otra autoridad judicial, o bajo su supervisión, o de otro modo, sean emitidas bajo supervisión independiente". Cuando las Partes en el Convenio no hagan tal declaración, se exigirá a los proveedores de servicios que respondan a las órdenes de presentación de las autoridades policiales transfronterizas sin ningún tipo de supervisión judicial. El hecho de que la recuperación de la información de los abonados en general no requiera validación judicial es contrario a la reciente sentencia del Tribunal Europeo de Derechos Humanos (TEDH) en el caso Benedik c. Eslovenia[4], en el que se consideró que se había violado el artículo 8 en relación con el hecho de que la policía eslovena no obtuviera una orden judicial antes de acceder a la información de los abonados asociada a una dirección IP dinámica. Según el Tribunal, la disposición legal utilizada por la policía eslovena para acceder a la información de los abonados asociada a una dirección IP dinámica sin obtener previamente una orden judicial no cumplía la norma del Convenio de ser "conforme a la ley".
2. Garantizar que, tras una orden de presentación, **los datos se transferirán al país solicitante sólo después de que se haya notificado a una autoridad competente e independiente de la Parte**. **En la sección 4.1 párrafo 5.a** se deja a la entera discreción de las Partes en el Convenio la obligación de exigir a la Parte emisora que le notifique simultáneamente cualquier orden enviada directamente a un prestador de servicios en su territorio, ya sea en todo momento o en circunstancias determinadas. De la misma manera, no es obligatorio que las Partes del Convenio exijan a los proveedores de servicios que consulten a las autoridades de la Parte en circunstancias identificadas antes de la divulgación (**Sección 4.1 párrafo 5.b).**
3. **Garantizar unos requisitos y motivos suficientes para denegar la ejecución de órdenes de**

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

producción internacionales, incluida la ausencia de **doble tipificación penal** o el hecho de que los datos solicitados estén amparados por el **secreto profesional**. Esto último debe indicarse explícitamente en la **sección 4.1, apartados 5.a y 5.b**, y constituye un motivo absoluto de denegación de la ejecución de una orden. CCBE desea subrayar que el secreto profesional puede abarcar no sólo los datos de contenido, sino también otros tipos de datos (por ejemplo, los datos de tráfico y, en determinadas circunstancias, la información de los abonados). Además, es necesario tener en cuenta la circunstancia de que cuando se busca la recuperación de los datos de los abonados, a menudo es el precursor de otras actividades de investigación. Cuando los datos se refieran a abogados, su recuperación supondrá un riesgo sustancial de violación del secreto profesional de las comunicaciones con sus clientes, e incluso cuando los datos de los abonados se refieran a personas que no sean abogados, puede existir el riesgo de que una investigación posterior conduzca a una infracción de las comunicaciones privilegiadas. Para protegerse de estos peligros, se requiere validación y supervisión judicial. Por otra parte, en cuanto a los procedimientos contenciosos (litigios penales o civiles), cualquier violación del secreto profesional constituye per se una violación del derecho a un juicio justo con arreglo al artículo 6 del CEDH y, como tal, debe reconocerse como motivo único y suficiente para rechazar la ejecución de una orden de presentación. En este momento, el proyecto de disposiciones no ofrece ningún motivo de denegación para los prestadores de servicios.

4. Garantizar que la autoridad competente informe al proveedor de servicios destinatario que esté tratando los datos solicitados sobre los recursos legales existentes, tales como los motivos de denegación.

5. Garantizar que la imposición de **restricciones de confidencialidad** a las órdenes de presentación esté **sujeta a la aprobación de una autoridad judicial independiente** y que en cada caso esté debidamente motivada y justificada por la autoridad de expedición sobre la base de evaluaciones significativas y documentadas.

6. Garantizar que las restricciones de confidencialidad no se prolonguen más allá de lo estrictamente necesario. **Cuando cesen las restricciones de confidencialidad, se debe informar a los interesados y poner a su disposición los recursos legales adecuados**.

7. Garantizar que los sospechosos o acusados, o sus abogados, puedan solicitar la emisión de órdenes internacionales de producción o conservación con la misma eficacia que las autoridades encargadas de hacer cumplir la ley, a fin de garantizar la observancia del **principio de igualdad de armas** entre la acusación y la defensa, sin lo cual el acusado se encuentra en una situación de desventaja significativa.

8. **Garantizar que las órdenes de producción dirigidas a la información de los abonados sólo puedan emitirse en caso de delitos graves**. Difícilmente puede justificarse que las órdenes dirigidas a la información de los abonados puedan emitirse también para delitos menores y no se limiten a delitos graves. Esto parece entrar en conflicto con las sentencias del Tribunal de Justicia de las Comunidades Europeas en el asunto Tele2/Watson[5] Tele2/Watson y Digital Rights Ireland[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.