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

Posición de CCBE sobre la propuesta de Reglamento de la Comisión sobre las Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal

19/10/2018

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. CCBE responde regularmente en nombre de sus miembros a cuestiones normativas que afectan a los ciudadanos y abogados europeos.

El 14 de abril de 2018, la Comisión Europea publicó una propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas en materia penal.

CCBE agradece que la Comisión haya tenido en cuenta diversos aspectos que CCBE sugirió durante el proceso de consulta anterior. CCBE emitió previamente comentarios preliminares sobre el tema que se pueden consultar para obtener más detalles[1]. Con este documento, CCBE desea ampliar su posición en relación con una serie de aspectos de la propuesta.

1. Base jurídica, necesidad y proporcionalidad.

La pregunta clave que surge de esta iniciativa legislativa es si el artículo 82(1) del Tratado de Funcionamiento de la Unión Europea (TFUE) constituye la base jurídica adecuada para un instrumento que permite a las autoridades policiales de un Estado miembro obligar a las empresas que ofrecen comunicaciones electrónicas y/o servicios de la sociedad de la información en la UE para conservar y/o entregar la prueba electrónica, independientemente de la jurisdicción dónde se ubique la empresa y dónde se almacenen los datos.

El principio de reconocimiento mutuo al que se refiere el artículo 82 suele entenderse como reservado únicamente a la cooperación entre las autoridades judiciales. Sin embargo, la propuesta prevista no involucra a las autoridades policiales o judiciales del Estado miembro en que se encuentre la empresa que recibe la solicitud. En cambio, la propuesta busca conferir una jurisdicción extraterritorial a la policía o las autoridades judiciales de un Estado miembro directamente para dirigirse a una entidad privada en otro Estado miembro. Además, el Reglamento propuesto también implica la ejecución transfronteriza del EPOC[2] y EPOC-PR[3] que han sido emitidos y validados solo por los fiscales y, por lo tanto, no son decisiones judiciales.

---

[1] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20180629_CCBE-Preliminary-comments-on-the-Commission-proposal-for-a-Regulation-on-European-Production-and-Preservation-Orders-for-electronic-evidence-in-criminal-matters.pdf

[2] EPOC significa "Certificado de Orden Europea de Entrega".

[3] EPOC-PR significa "Certificado de Orden Europea de Conservación".

En vista de estas circunstancias, CCBE considera que no es posible, sobre la base jurídica declarada, que las instituciones de la UE adopten un instrumento legal que permita a las autoridades nacionales de un Estado miembro ordenar la presentación de pruebas electrónicas a entidades privadas de otra jurisdicción. Además, es dudoso que la base jurídica seleccionada sea suficiente para adoptar el proyecto del artículo 13 de la propuesta que obliga al Estado Miembro a establecer sanciones pecuniarias por violaciones de las obligaciones establecidas en los Artículos 9-11.

CCBE también considera que la elección de un Reglamento en lugar de una Directiva como instrumento jurídico podría conducir a un cambio de paradigma en el área del Derecho penal que implicaría un alto riesgo de que la legislación de la UE disminuya los estándares nacionales más altos. A este respecto, también es conveniente señalar que las medidas relativas a la armonización de procedimientos para facilitar, entre otras cosas, la admisibilidad mutua de las pruebas entre los Estados miembros, pueden adoptarse, de conformidad con el artículo 82 (2), únicamente mediante directivas.

Otra pregunta importante es hasta qué punto la propuesta tiene algún valor añadido en comparación con los Acuerdos de Asistencia Judicial Mutua (MLAT), así como con la Orden Europea de Investigación (EIO) y si está acompañada de suficientes garantías. En otras palabras, ¿es el instrumento previsto realmente necesario para lograr su propósito y proporcional al objetivo que pretende alcanzar?

Según el memorando explicativo, parece que el objetivo principal de la propuesta es hacer que la obtención y recopilación de las pruebas electrónicas almacenadas en otra jurisdicción sea más rápida al eludir (a menudo sin recursos) a las autoridades judiciales nacionales en el Estado miembro donde se almacenan las pruebas. Como tal, la propuesta esencialmente introduce un mecanismo a través del cual los sistemas establecidos de asistencia judicial se pasan por alto y la protección de los derechos fundamentales se delega parcial o totalmente a las partes privadas. CCBE no está de acuerdo con este enfoque, ya que socava los deberes esenciales de las autoridades judiciales nacionales de garantizar que los derechos de sus ciudadanos no se vean comprometidos o socavados. Tal socavación sí surge, debido a que ya no sería posible que las autoridades judiciales nacionales realicen un control legal de las solicitudes de cooperación judicial que emanan de la autoridad de otro Estado miembro. Por lo tanto, CCBE considera que, en lugar de restringir el papel y las responsabilidades de las autoridades judiciales nacionales, un enfoque más apropiado sería hacer que los procedimientos de MLA y EIO sean más rápidos a través de la digitalización y su mejor equiparación a las autoridades nacionales para responder a las solicitudes transfronterizas. Sin algún tipo de verificación de legalidad por parte de las autoridades judiciales relevantes del estado miembro en el que se encuentra la empresa, existe el riesgo de que se le exija a la empresa que haga una divulgación de una naturaleza que normalmente no podría ser requerida en la jurisdicción donde se buscan los datos. Las entidades más pequeñas pueden carecer de los recursos legales y la experiencia para consultar la legalidad de la orden de entrega.

Además de la necesidad de una verificación de legalidad de la orden de entrega por parte de las autoridades judiciales competentes del país donde se buscan los datos, también podría ser necesaria la participación en los procedimientos de una persona o entidad que tenga conocimiento de asuntos tales como como si es probable que la prueba esté cubierta por la confidencialidad abogado-cliente. Normalmente ese sería el controlador de datos (por ejemplo, un despacho de abogados). Se

agradece que esto no siempre sea apropiado, especialmente cuando existe un riesgo de destrucción de la prueba. Sin embargo, una vez que se hayan asegurado los datos, sería posible y apropiado realizar una verificación de legalidad antes de la entrega de los datos específicos.

Por tanto, CCBE propone restringir el ámbito de la propuesta para que se relacione únicamente con las órdenes de conservación. Para la entrega de prueba electrónica, una orden de conservación podría estar seguida del lanzamiento de una Orden Europea de Investigación o con un procedimiento bajo un Acuerdo de asistencia judicial mutua. Otro argumento a favor de restringir la propuesta de las órdenes de conservación es la incertidumbre técnica y de procedimiento con respecto a la ejecución de órdenes de entrega dirigidas a entidades privadas en otra jurisdicción sin la participación de las autoridades donde se buscan los datos, incluyendo:

- ¿Cómo se debe servir el EPOC a los destinatarios (por correo certificado, electrónicamente, 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 garantizar que los datos sean veraces, precisos y sin restricciones?

- ¿Cómo pueden evaluar a los destinatarios la autenticidad y legalidad de los EPOC?

Como consecuencia de las cuestiones señaladas anteriormente, CCBE sostiene que la propuesta debería tener un ámbito restringido sobre las órdenes europeas de conservación y que los objetivos perseguidos por la Comisión podrían alcanzarse igualmente utilizando, en combinación con la creación de una orden europea de conservación, los procedimientos previstos en la EIO y el MLAT que, en consecuencia, también podrían requerir mejoras.

No obstante, en caso de que las instituciones europeas decidieran seguir adelante con la propuesta tal como está actualmente, CCBE presentaría algunas observaciones adicionales y sugerencias para enmendar la propuesta como se detallan a continuación.

2. Revisión judicial en el Estado miembro de ejecución

Sería necesaria alguna forma de revisión judicial en el Estado de ejecución para garantizar una protección suficiente de los derechos fundamentales. Por tanto, CCBE sugiere que se utilicen las disposiciones del artículo 11(1) de la Directiva EIO 2014/41 sobre los motivos de no reconocimiento o no ejecución de la Orden. Si compromete las investigaciones para notificar al sujeto de los datos antes de que se entreguen, al menos se debe realizar una revisión judicial significativa en el Estado miembro de ejecución sobre la legalidad de la medida de acuerdo con la legislación de ese estado. Alternativamente, se podría considerar **la creación de un órgano judicial a nivel europeo compuesto por autoridades de todos los Estados miembros y expertos independientes (jueces y abogados), a los que se les podría exigir que den luz verde a todas las órdenes dirigidas a proveedores de servicios y otras entidades** (similares, por ejemplo, al artículo 15 del Proyecto de Instrumento Legal sobre Vigilancia y Privacidad dirigido por el gobierno). La importancia de un mecanismo de revisión

judicial para salvaguardar los derechos fundamentales ya está reconocida en los instrumentos europeos, por ejemplo, el Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, que implementa una mayor cooperación en el establecimiento de la Oficina de la Fiscalía Europea ("EPPO").

3. Objeto

El **artículo 1(1)** establece que el reglamento se refiere a la obtención y conservación transfronteriza de las pruebas electrónicas sin especificar qué se entiende por pruebas. Para evitar cualquier diferencia en la interpretación sobre el tema del instrumento propuesto, es necesario que el **Artículo 2** incluya una definición clara de lo que se considera prueba. La definición podría formularse de la siguiente manera:

- "Todos los datos que podrían ser potencialmente utilizados en los tribunales en relación con un caso penal específico con el propósito de que se presenten como prueba los hechos alegados que son importantes para el caso".

4. Ámbito

CCBE considera que es de suma importancia que las órdenes de entrega y conservación deban cumplir con los requisitos de necesidad y proporcionalidad. En consecuencia, el **EPOC y el EPOC-PR deberían emitirse solo en relación con delitos específicos y no deberían emitirse con el propósito de monitorear supuestas actividades delictivas.**

En el considerando 29 se estipula que una orden europea de entrega solo debe emitirse si es necesaria y proporcionada. La evaluación debe tener en cuenta si la Orden se limita a lo que es necesario para lograr el objetivo legítimo de obtener los datos relevantes y necesarios para que sirvan como prueba en el "caso individual solamente". Sin embargo, en el texto sustantivo del reglamento propuesto no existen criterios específicos para la prueba de necesidad y proporcionalidad. Por ejemplo, las condiciones para emitir los EPOC/EPOC-PR no incluyen ningún umbral de un grado suficiente de sospecha. **Para evitar abusos, las autoridades competentes deben validar la EPO solo si existen razones de peso que den lugar a un grado suficiente de sospecha para justificar la incautación de datos a través de la frontera.**

Además, el **Artículo 3(2)** estipula que las Órdenes europeas de entrega y de conservación (téngase en cuenta que en el texto "entrega" aparece dos veces, con la referencia a la "conservación" desaparecida) solo pueden emitirse para "procedimientos penales", tanto durante la fase previa al juicio y la fase de la prueba. Asimismo, en el **artículo 5(2)** se recuerda que las órdenes europeas de entrega deben ser necesarias y proporcionadas a los efectos del procedimiento a que se refiere el artículo 3(2). Sin embargo, consideramos que la redacción del artículo 3(2) podría interpretarse de una manera que sea inconsistente con la redacción del Considerando 29, que se refiere a la necesidad de que los EPOC se emitan con el propósito de un "caso individual solamente". Teniendo en cuenta la materia establecida en el artículo 2, también es necesario especificar que el ámbito de la propuesta debe ser, y esto se limita a la obtención y conservación transfronteriza de pruebas electrónicas, en lugar de que se aplique más ampliamente a la entrega y conservación de datos electrónicos en general.

Por tanto, CCBE propone que se modifique la redacción del artículo 3(2) aclarando que las órdenes solo pueden emitirse con el fin de obtener la prueba en el curso de un proceso penal específico. La disposición adecuada sería la siguiente: "Las órdenes europeas de entrega y las órdenes europeas de entrega solo pueden emitirse ***con el fin de obtener pruebas en el curso de procedimientos penales específicos***, tanto durante la fase previa al juicio como durante la fase de prueba".

5. Responsabilidad

Según el considerando 46, siempre que los proveedores de servicios actúen de buena fe, no se les puede responsabilizar de los daños causados por una ejecución incorrecta o injustificada de un EPOC o EPOC-PR. Creemos que una exención de responsabilidad tan amplia podría ser problemática en el caso de que, por ejemplo, la información privilegiada se comparta erróneamente con las autoridades judiciales. Dicha exención de responsabilidad podría llevar a una situación en la que los proveedores de servicios ejecutan automáticamente las solicitudes sin un análisis adecuado.

Por tanto, CCBE considera que el considerando debe ser más específico, especialmente en lo que se refiere a lo que significa "buena fe".

6. Validación judicial

No parece haber una justificación adecuada de por qué una Orden Europea de Entrega (EPO) para los datos de suscriptor y acceso en general no requiere validación judicial. Debe establecerse con mayor claridad qué tipo de datos se incluyen en la clase de “suscriptor o datos de acceso” para evitar la incautación de información que normalmente requeriría una supervisión judicial independiente de acuerdo con las normas nacionales, los procedimientos de MLA o la Orden Europea de Investigación (EIO).

Por ejemplo, las direcciones IP o las interfaces se encuentran en más de una categoría, es decir, datos de acceso y datos de suscriptor **(artículo 2 (7) (b))**. Además, la definición de datos de suscriptor incluye no solo lo que generalmente se entiende por datos de suscriptor (consulte el artículo 2 (7) (a)), sino también términos genéricos amplios como "el tipo de servicio [...] que incluye datos técnicos y datos que identifiquen medidas técnicas relacionadas o interfaces [...] y datos relacionados con la validación del uso del servicio "(artículo 2 (7) (b)). Incluso se podría considerar que estos términos generales incluyen datos que no están relacionados con el significado habitual del término "tipo de servicio", como, por ejemplo, cualquier característica técnica del servicio prestado, borrando así la distinción entre datos de acceso y suscriptores. Teniendo en cuenta también que la nueva regulación de privacidad electrónica[4] propuesta utiliza otro tipo de clasificación (contenido de comunicaciones electrónicas y metadatos), y también que la Directiva de privacidad electrónica actualmente vigente[5] utiliza otra definición más de datos de tráfico para aproximadamente los mismos propósitos, conduce a una situación confusa donde existen definiciones superpuestas y

[4] Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de datos personales en las comunicaciones electrónicas y por la que se deroga la Directiva 2002/58 / CE.
[5] Directiva 2002/58 / CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de datos personales y la protección de la privacidad en el sector de las comunicaciones electrónicas.

potencialmente competitivas. En estas circunstancias, existe una necesidad apremiante de garantizar la claridad y la coherencia de la definición, limitando el número de dichos términos al mínimo necesario.

El hecho de que la recuperación de los datos de acceso y suscriptor en general no requiera validación judicial también va en contra de la reciente sentencia del TEDH en el caso de Benedik c. Eslovenia[6], donde se consideró que había habido una violación del artículo 8 CEDH en relación con el hecho de que la policía eslovena no obtuviera una orden judicial antes de acceder a la información del suscriptor asociada con una dirección IP dinámica. Según el TEDH, la disposición legal utilizada por la policía eslovena para acceder a la información del suscriptor asociada con una dirección IP dinámica sin obtener primero una orden judicial no cumplía con el estándar del CEDH de estar "de acuerdo con la ley".

En el caso Tele2/Watson[7], el TJUE sostuvo que “es esencial que el acceso de las autoridades nacionales competentes a los datos retenidos, como norma general, excepto en casos de urgencia establecida de manera válida, debe estar sujeto a una revisión previa realizada por un tribunal o por un órgano administrativo independiente, y que la decisión de ese tribunal u órgano se tome después de una solicitud razonada de las autoridades presentadas, en otras, en el marco de los procedimientos de prevención, detección o enjuiciamiento del delito "(párrafo 120). Esto plantea la siguiente pregunta:

- ¿Cómo pueden las autoridades de validación evaluar adecuadamente la conveniencia de una solicitud para emitir una EPO?
- ¿Qué información recibirán aparte del formulario de certificado?
- ¿Debería dejarse esto a cada Estado miembro nacional para que lo especifique o debe haber algunos criterios y normas comunes?

Es importante aclarar que el secreto profesional/privilegio profesional legal puede cubrir no solo los datos de contenido, sino también otro tipo de datos, por ejemplo, datos de acceso, y en tales casos, se requiere validación y supervisión judicial.

Si el Reglamento no proporciona una certeza absoluta sobre qué tipo de datos se encuentran en las distintas categorías de datos, las autoridades policiales (LEA) no sabrán si necesitan validación judicial, y los destinatarios no podrán evaluar si las EPO se han emitido legalmente.

Además, podría ser necesaria la participación en los procedimientos de una persona que tenga conocimiento de cuestiones tales como si es probable que la prueba esté cubierta por la confidencialidad abogado-cliente. Normalmente ese sería el controlador de datos. Se agradece que esto no siempre sea apropiado, especialmente cuando existe un riesgo de destrucción de la prueba.

Por tanto, CCBE sugiere que los EPOC para los datos de suscriptor y acceso, deben ser emitidos y validados por un juez, tribunal o juez de instrucción y que se podría requerir un proceso de dos etapas, siendo la primera etapa el uso de una orden de conservación para asegurar la prueba antes

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

[7] 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

de cualquier solicitud impugnada de una orden de entrega y la segunda etapa podría ser la audiencia (si se impugna) de la solicitud de una orden de entrega.

7. Condiciones para la emisión de un Certificado de Orden europea de entrega.

Requisito de la doble criminalidad

En la segunda parte de los **artículos 3(2) y 5(2),** solo en relación con los delitos punibles en el Estado miembro de emisión se puede emitir un EPOC. **CCBE sostiene que debe exigirse que el delito en cuestión sea punible tanto en el Estado de emisión como en el Estado miembro donde se buscan los datos.**

Los datos de suscriptores o de acceso de la EPO

Tampoco puede justificarse que las Órdenes europeas de entrega dirigidas a datos de suscriptores o datos de acceso también puedan emitirse para delitos menores y no se limiten a delitos graves (artículo 5 (3)). Esto parece estar en conflicto con las decisiones del TJUE en el caso de Tele2/ Watson[8] y Derechos Digitales Irlanda[9]. **Por tanto, CCBE propone que los datos de suscriptores o los datos de acceso de una EPO dirigidos solo se puedan emitir para delitos graves.**

Condiciones para los datos transaccionales o de contenido de la EPO

Para los datos transaccionales o de contenido de la EPO, surge la pregunta de si una sentencia de custodia de un máximo de al menos 3 años es lo suficientemente alta como para evitar que el instrumento sea objeto de abuso para abordar pequeños delitos. Según los códigos penales de los Estados miembros, un gran número de delitos se incluyen en esta categoría, incluidos los delitos que no se consideran como un delito grave. Los delitos punibles de menos de 3 años también podrían cubrirse si entran en el ámbito de aplicación de cualquiera de los artículos mencionados de la Decisión marco 2001/413/JAI del Consejo, la Directiva 2011/93/UE, la Directiva 2013/40/UE, la Directiva (UE) 2017/541 (artículo 5 (4)). La extensión del ámbito a todos los asuntos con una sentencia máxima de al menos tres años no hace justicia a la severidad de la interferencia. A CCBE le preocupa que esto sea muy probable que se aplique a delitos menores en muchos Estados miembros. Por tanto, propone incluir una lista de delitos específicos que deben limitarse a delitos graves solo según lo prescrito en las decisiones del TJUE.

Destinatarios de las órdenes europeas de entrega

Al responder a la consulta pública sobre la prueba electrónica, CCBE hizo hincapié en que cuando se hace cumplir una orden de entrega, se debe notificar a una organización, permitirle evaluar sus derechos y obligaciones legales y, si es posible, ser capaz de impugnar la solicitud antes de que cualquier dato pueda ser incautado.

Esto implica que las solicitudes de acceso a la prueba digital deben, siempre que sea posible, dirigirse siempre a los controladores de datos, en lugar de a los procesadores de datos, que, especialmente cuando los datos están controlados por una firma de abogados, brindan mejores garantías contra cualquier intercambio ilegal de datos de información privilegiada. Los procesadores de datos u otros

---

[8] 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

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

intermediarios no tendrían información sobre muchos aspectos importantes del contexto de los datos que se han buscado y, por tanto, no siempre estarían en condiciones de evaluar la legalidad de la solicitud o cualquier otro requisito legal que sea necesario sentirse satisfecho.

El Reglamento propuesto deja claro en el **artículo 5(6)** que, cuando una Orden Europea de Entrega apunta a los datos de una empresa u otra entidad que no sea una persona física, los datos deben solicitarse en primera instancia a esa entidad, a menos que hacerlo socavaría la investigación.

Esta protección es importante, ya que los controladores de datos generalmente están en la mejor posición para revisar y hacer valer cualquier derecho que se adjunte a la prueba electrónica que deben entregar.

Los despachos de abogados están cubiertos por esta disposición y, por tanto, deben tratarse directamente para que puedan evaluar los requisitos legales para cumplir con dichas solicitudes de datos, incluido el hecho de que los datos solicitados estén sujetos a secreto profesional. Por tanto, esta exención es especialmente crítica en los casos en que los datos solicitados están en manos de un despacho de abogados.

Sin embargo, CCBE está preocupado por la redacción muy general que proporciona a las autoridades policiales con un margen muy amplio para eludir a los controladores de datos. Además, este artículo solo se aplica a las empresas, mientras que en la mayoría de las jurisdicciones, los profesionales independientes (que constituyen la gran mayoría de las prácticas legales europeas) no se consideran personas legales. Por tanto, los abogados ejercientes únicos que son personas físicas no estarían sujetos a la misma protección que los despachos de abogados. Independientemente de cómo se organiza una práctica (profesional único o despacho de abogados), el secreto profesional siempre debe estar protegido, y todas las garantías necesarias deben garantizarse.

En consecuencia, CCBE propone que se especifique en el artículo 5(6) que la autoridad emisora está obligada a establecer y justificar debidamente en cada caso por qué no se puede enviar un EPOC al controlador de datos (es decir, compañía, entidades distintas de las personas físicas y profesionales regulados) sobre la base de evaluaciones significativas y documentadas. Además, el término "profesionales regulados" debe agregarse en la misma disposición.

Si bien el artículo 5(6) estipula que cuando una EPO apunta a los datos de una compañía u otra entidad que no sea una persona física, los datos deben solicitarse en primera instancia a esa empresa, no está claro en el texto sustantivo del Artículo 5(6) ni del considerando 34 mediante qué tipo de medida de investigación deben solicitarse los datos en poder de dichas entidades. En el memorando explicativo se indica que "[t] este puede requerir un procedimiento de EIO o MLA en el que la empresa no sería un proveedor de servicios cubierto por el ámbito de este Reglamento". **Para evitar cualquier duda sobre esto, es necesario aclararlo en el texto sustantivo del Reglamento propuesto.**

Las órdenes europeas de entrega que cubren información privilegiada no deben ser emitidas ni ejecutadas

Otra cuestión clave es que debe quedar exento del ámbito del instrumento legislativo, los datos que la autoridad requirente conoce o debería conocer están protegidos por obligaciones de secreto profesional/privilegio profesional legal según la ley de emisión y/o ejecución del Estado.

El **artículo 5(7)** establece que, en caso de que existan razones para creer que los datos solicitados están cubiertos por el secreto profesional, debe solicitarse una aclaración contactando a las autoridades competentes antes de proceder con la solicitud. Si los datos están cubiertos por obligaciones de secreto profesional, la EPO no debe emitirse.

Sin embargo, la pregunta surge sobre cómo las LEA pueden determinar quién es un abogado, especialmente si es un abogado en otro Estado miembro. Se requieren medidas técnicas adecuadas para garantizar que tanto las LEA como los proveedores de servicios sepan cuándo los abogados son titulares de los datos (y esto puede implicar algún medio de verificación de la identidad de los abogados). Una forma pragmática sería exigir a los proveedores de servicios que ofrezcan a los abogados una opción para indicar dicha información; por supuesto, solo después de una verificación cuidadosa de si ese usuario es realmente un abogado, como se afirma.

A este respecto, CCBE podría ayudar a crear un mecanismo para identificar abogados sobre la base de la herramienta prototipo desarrollada en el marco del proyecto FAL2 para la identificación de abogados. Esta herramienta (que también se está utilizando en el contexto del sistema e-CODEX) podría adaptarse para este propósito específico.

Además, aunque el secreto profesional/privilegio profesional legal es un motivo para rechazar la validación judicial (y debe tenerse en cuenta durante un juicio penal, ver Artículo 18), no es un motivo explícito para negarse a ejecutar una EPO. **Por tanto, debe especificarse en el artículo 9 que el hecho de que los datos solicitados estén cubiertos por el secreto profesional constituye un motivo válido para rechazar la ejecución de una EPO. Además, en el formulario (en anexo), se debe añadir una casilla adicional sobre secreto profesional como razón para rechazar la ejecución de una EPO.**

8. Condiciones para emitir un Certificado de Orden Europea de Conservación

El **artículo 6(2)** estipula que se puede emitir una orden de conservación cuando sea necesario y proporcional para evitar la retirada, eliminación o alteración de los datos ante una solicitud posterior de entrega de estos datos a través de asistencia judicial mutua, una Orden Europea de Investigación o una Orden europea de entrega. Se pueden emitir Órdenes Europeas de Conservación para preservar los datos de todos los delitos". Sin embargo, carece de garantías contra la Conservación general e indiscriminada de los datos (ver casos Tele2/Watson y Derechos digitales Irlanda). Tampoco hay garantías contra órdenes de conservación recurrentes que no sean seguidas por órdenes de entrega.

Por lo tanto, esta disposición debe ponerse en línea con la decisión del TJUE en Tele2/Watson (véanse los párrafos 108-111). Una posible solución sería especificar que un EPOC-PR tenga que ver con la retención específica de datos, con el fin de combatir delitos graves, siempre que la retención de datos sea limitada con respecto a las categorías de datos que deben conservarse, los medios de comunicación afectados, las personas interesadas y el período de retención adoptado, a lo estrictamente necesario.

9. Ejecución de un Certificado de Orden Europea de Conservación

Siguiendo la redacción del **artículo 10**, la obligación del destinatario de preservar los datos solicitados deja de existir después de 60 días, a menos que la autoridad emisora haya confirmado que una Orden Europea de Entrega posterior ha sido "lanzada", aunque aún no se haya "cumplido". En tal situación, no se ha proporcionado un límite de tiempo para la Conservación de los datos solicitados.

En consecuencia, CCBE considera que es necesario incluir un límite de tiempo para los casos en que la autoridad emisora, por cualquier motivo, se abstenga de cumplir la Orden Europea de Entrega.

10. Motivos de denegación para ejecutar un Certificado de Orden Europea de Entrega y un Certificado de Orden Europea de Conservación

CCBE considera que los motivos para negarse a ejecutar un EPOC son demasiado restrictivos. Aparte de razones técnicas o prácticas (por ejemplo, el EPOC está incompleto o el destinatario no puede cumplir debido a fuerza mayor), el único motivo de no ejecución que puede ser invocado por el destinatario es que si considera que "con base en la única información contenida en el EPOC es evidente que viola manifiestamente la Carta de los Derechos Fundamentales de la Unión Europea o que es manifiestamente abusiva". **Por tanto, se deben establecer otros motivos específicos para rechazar la ejecución de una EPO, incluida (como se mencionó anteriormente) la ausencia de doble criminalidad o el hecho de que los datos solicitados están cubiertos por el secreto profesional.**

En cuanto a los procedimientos contenciosos (litigios penales o civiles), cualquier violación del secreto profesional es per se una violación del derecho a un juicio justo de acuerdo con el artículo 6 del CEDH y debe, como tal, debería reconocerse como un motivo único y suficiente para rechazar la ejecución de una EPO.

11. Notificación al interesado.

El requisito de notificación establecido en el **artículo 11(2)** puede ser fácilmente ignorado por las autoridades ya que siempre hay una razón para descubrir por qué tal notificación podría poner en peligro la investigación/los procedimientos. Esto socava gravemente los derechos de las personas a un juicio justo, ya que, mientras esas personas no sepan que se han tomado sus datos, no pueden hacer valer sus derechos. **CCBE considera que la imposición de restricciones de confidencialidad a los EPOC debe estar sujeta a la aprobación de una autoridad judicial independiente y, en cada caso, debe estar debidamente motivada y justificada por la autoridad emisora sobre la base de evaluaciones significativas y documentadas. Con respecto a las órdenes europeas de conservación, CCBE también sostiene que la autoridad emisora debe estar obligada a informar al interesado.**

12. Los derechos de la defensa.

Cualquier propuesta para la recuperación de pruebas electrónicas no debe considerarse únicamente relacionada con el procesamiento. Deben tenerse debidamente en cuenta los derechos de defensa.

La propuesta no tiene en cuenta debidamente el requisito de la igualdad de condiciones en los procedimientos penales, que es un concepto reconocido por el TEDH en el contexto del derecho a un juicio justo. Mientras que los fiscales pueden emitir órdenes de entrega y conservación, no existen disposiciones que permitan a los acusados o sus representantes acceder o solicitar pruebas electrónicas.

Además, la propuesta no proporciona ningún requisito u orientación para que los destinatarios limiten la transmisión de pruebas electrónicas a datos que sean relevantes para los fines del proceso penal. Como resultado, las LEA podrían verse abrumadas por los datos. Tampoco existe ninguna disposición para garantizar que los demandados no se sobrecarguen a su vez por el peso de las pruebas electrónicas, o que dichas pruebas electrónicas sean fácilmente accesibles mediante la adición de metadatos apropiados, como un índice y un índice de contenidos. Sin la ayuda de tales metadatos, es muy difícil o incluso imposible para los abogados hacer valer los derechos de sus clientes.

CCBE sostiene que, al igual que con el EIO, las personas sospechosas o acusadas o sus abogados deberían poder solicitar la emisión de una Orden Europea de Entrega o Conservación de la misma manera que los fiscales. Si no, la propuesta socava el principio de igualdad de condiciones entre la fiscalía y la defensa, colocando al acusado en una desventaja significativa. Además, las entidades a las que se dirigen deben estar obligadas a entregar solo los datos que son relevantes para los fines de la investigación penal.

13. Recursos efectivos y revisiones judiciales.

Con respecto al **artículo 17**, CCBE considera que **las personas afectadas por un EPOC no solo deben poder ejercer sus recursos ante el tribunal en el estado de emisión, sino también en el tribunal del Estado miembro donde se buscan los datos. CCBE considera que también es necesario extender el derecho a la reparación efectiva del artículo 17 a las Órdenes Europeas de Conservación**