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

Comentarios preliminares de CCBE sobre la propuesta de Comisión para el Reglamento sobre las Órdenes Europeas de Entrega y Conservación de pruebas electrónicas a efectos de enjuiciamiento penal

29/06/2018

El Consejo de la Abogacía Europea (CCBE) representa a las Abogacías de 45 países, y a través de ellas, a más de 1 millón de abogados europeos. CCBE responde regularmente en nombre de sus miembros en cuestiones normativas que afectan a los ciudadanos y abogados europeos.

El 14 de abril de 2018, la Comisión Europea publicó una propuesta de Reglamento relativa a las Órdenes Europeas de Entrega y Conservación de pruebas electrónicas a efectos de enjuiciamiento penal.

CCBE agradece que la Comisión haya tenido en cuenta diversos aspectos que CCBE sugirió durante el proceso de consulta anterior. Con este documento, CCBE desea compartir sus observaciones iniciales en relación a una serie de aspectos de la propuesta. A su debido tiempo, presentará un posicionamiento más detallado.

La cuestión clave que surge de esta iniciativa legislativa es si la propuesta de mejorar los poderes de acceso a la prueba electrónica a través de las fronteras nacionales por parte de las autoridades investigadoras, va acompañada de las suficientes garantías procesales y los trámites de diligencia debida. En otras palabras, ¿hay algún aspecto que pueda menoscabar los derechos en un juicio justo?, y, de ser así, ¿cómo podrían abordarse estos aspectos?

Hay tres cuestiones centrales dentro de las cuales se encuentran la mayoría de las observaciones detalladas:

1. La disposición de un mecanismo efectivo que garantice la protección de las comunicaciones abogado-cliente. Esta plantea, en particular, los siguientes problemas:

    a) ¿Sobre qué personas deben ejercerse las Órdenes?

    b) ¿Cuán lejos es necesario el examen judicial de las solicitudes?

    c) ¿Cómo se puede asegurar la efectividad de dicho examen?

    d) ¿Es necesario complementar los motivos de la denegación propuestos?

    e) ¿Las disposiciones para la notificación requieren ser complementadas?

2. Garantizar la igualdad de medios entre la acusación y la defensa.

3. Provisión de una revisión judicial efectiva

El siguiente análisis contiene ciertas observaciones preliminares sobre estas y otras cuestiones. Se acepta que estas observaciones son probablemente el primer paso en un proceso dinámico y colaborativo al abordar el texto de la Propuesta en el curso del proceso legislativo, y debe verse como un documento preliminar. CCBE presentará observaciones más completas y detalladas a medida que avance el proceso legislativo.

1. Protección de la confidencialidad de la comunicación abogado-cliente

Para que los abogados sean eficaces en la defensa de los derechos de sus clientes, debe haber confianza en que las comunicaciones entre cliente y abogado se mantengan confidenciales. Este principio - generalmente conocido como "secreto profesional" es reconocido por todos los países de la UE y ha sido confirmado por el TJUE y el TEDH en numerosas sentencias. La violación del secreto profesional constituye en algunos Estados miembros de la UE no solo una violación de un deber profesional, sino también una infracción penal.

El material potencialmente privilegiado disfrutará de una mayor protección del artículo 8 del Convenio Europeo de Derechos Humanos (CEDH). Además, las comunicaciones abogado-cliente en relación con el procedimiento contencioso (litigios penales o civiles) también gozan de protección en virtud del artículo 6 del CEDH sobre el derecho a un proceso equitativo. Los derechos del artículo 6 (a diferencia de los derechos del artículo 8) son absolutos, en el sentido de que no se pueden aplicar limitaciones o excepciones.

Destinatarios de las Órdenes Europeas de Entrega

Al responder a la consulta pública sobre la prueba electrónica, CCBE enfatizó que cuando una orden de entrega es obligatoria, se debe notificar a una organización, se le debe permitir evaluar sus derechos y obligaciones legales, y si es posible, se debe ser capaz de desafiar la solicitud antes de que se pueda incautar cualquier información.

Esto implica que las solicitudes de acceso a la prueba digital deben, cuando sea posible, dirigirse siempre a los responsables de datos, en lugar de a los proveedores de los mismos que, especialmente cuando los datos sean gestionados por un despacho de abogados, proporcionaría mejores garantías contra cualquier intercambio ilícito de información privilegiada. Los responsables de datos, u otros intermediarios, no tendrían información sobre muchos aspectos importantes del contexto de los datos que se ha solicitado, y por lo tanto no siempre estaría en condiciones de evaluar la legalidad de la solicitud, o cualquier otro requisito legal que deba cumplirse.

El Reglamento propuesto deja claro en el **artículo 5(6)** que, cuando una Orden Europea de Entrega (EPO) contiene datos de una empresa, estos deberían buscarse en primera lugar en esa empresa, a menos que socaven la investigación.

Esta protección es importante ya que los responsables de los datos generalmente están en la mejor posición para revisar y afirmar cualquier derechos que se adjuntan a la prueba electrónica que se les solicita que entreguen.

Los despachos de abogados están cubiertos por esta disposición y, por tanto, deben abordarse directamente para que estén en condiciones de evaluar los requisitos legales para satisfacer tales solicitudes de datos, incluido el hecho de si los datos solicitados están sujetos al secreto profesional/privilegio profesional legal. 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, a CCBE le preocupa la redacción muy general, que brinda a las autoridades policiales un amplio margen para eludir aún a los responsables 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 los despachos de abogados europeos) no se consideran personas jurídicas. Por tanto, los abogados independientes que son personas físicas no estarían sujetos a la misma protección que los despachos de abogados. Por lo tanto, debe agregarse el término "profesionales regulados". Independientemente de cómo se organice un despacho (profesional independiente o despacho de abogados), el secreto profesional siempre debe estar protegido y todas las garantías procesales deben cumplirse en este sentido.

Las Órdenes Europeas de Entrega que cubren información privilegiada no deben emitirse ni ejecutarse

Otra cuestión clave es que los datos que la autoridad requirente sabe, o debería haber sabido, que están protegidos por la obligación del secreto profesional/privilegio profesional legal según la legislación del Estado de emisión y/o de ejecución están exentos del alcance del instrumento legislativo.

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

Sin embargo, surge la pregunta de cómo las autoridades encargadas de hacer cumplir la ley (LEA) pueden determinar quién es un abogado, especialmente si se trata de un abogado en otro Estado miembro. Algunas medidas técnicas parecen ser necesarias para garantizar que tanto las LEA como los proveedores de servicios sepan que los datos están en poder de los abogados (así como también cierta 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 tal información, por supuesto, solo después de una cuidadosa verificación de si ese usuario es realmente un abogado, como se afirmó.

En este sentido, CCBE podría ayudar a crear un mecanismo para identificar a los abogados sobre la base del prototipo desarrollado bajo el proyecto FAL2 para la identificación de abogados. Esta herramienta (que también se está utilizando en el contexto del sistema e-CODEX) se puede adaptar para este propósito específico.

Además, aunque el secreto profesional es un motivo para denegar la validación judicial (y debe tenerse en cuenta durante un juicio penal -véase el Artículo 18), no es un motivo explícito para denegar la ejecución de una EPO. Por lo tanto, debe especificarse en el artículo 9 que el hecho de que los datos solicitados estén cubiertos por el secreto profesional/el secreto profesional constituye un motivo válido para denegar la ejecución de una EPO. Además, en el formulario (en el Anexo), se debe agregar una casilla adicional sobre el secreto profesional como una razón para rechazar la ejecución de una EPO.

2. Validación judicial

Según CCBE, la validación judicial por parte del Estado requirente es la protección mínima que debe garantizarse, especialmente teniendo en cuenta que la orden ya no será verificada por la autoridad en el país requerido (como es el caso de los procedimientos de asistencia judicial mutua (MLA)).

Parece que no existe una justificación adecuada de por qué las EPO para suscriptores y los datos de acceso en general no requieren validación judicial. Es necesario establecer con mayor claridad qué tipo de datos se consideran 'suscriptores o datos de acceso' para evitar la confiscación de información que normalmente requeriría supervisión judicial independiente de conformidad con las normas nacionales, los procedimientos de asistencia judicial mutua o la Orden Europea de Investigación (EIO). Por ejemplo, las direcciones o interfaces IP caen en más de una categoría, es decir, datos de acceso y datos de abonado (**Artículo 2 (7) (b)**). Además, la definición de datos de suscriptor incluye no solo lo que generalmente se entiende bajo los datos del suscriptor (ver Artículo 2 (7) (a)), sino también términos muy genéricos como "el tipo de servicio [...] que incluye datos técnicos y datos que identifiquen medidas o interfaces técnicas [...] relacionadas y datos relacionados con la validación del uso del servicio "(Artículo 2 (7) (b)). Estos términos amplios podrían incluso incluir datos que no están relacionados con el significado habitual del término "tipo de servicio", como cualquier característica técnica del servicio prestado, borrando así la distinción entre los datos de acceso y los datos del suscriptor. Teniendo en cuenta también que la nueva regla propuesta de privacidad electrónica[1] utiliza otro tipo de clasificación (contenido de comunicaciones electrónicas y metadatos), y también considerando que la Directiva de privacidad electrónica actualmente vigente[2] utiliza otra definición más de datos de tráfico para aproximadamente los mismos propósitos, sería muy importante limitar el número de dichos términos al mínimo necesario.

Es importante aclarar que el secreto profesional puede abarcar no solo los datos de contenido, sino también otros tipos de datos, por ejemplo, acceder a los datos, y en tales casos, se requiere validación y supervisión judicial.

Si el Reglamento no proporciona certeza absoluta sobre qué tipos de datos se incluyen en las diversas categorías de datos, las LEA no sabrán si necesitan validación judicial, y los destinatarios no podrán evaluar si los EPO han sido emitidos legalmente.

3. Suficiente grado de sospecha

Las condiciones para emitir una Orden Europea de Entrega o Conservación no incluyen ningún umbral de suficiente grado de sospecha (Artículo 5). **Para evitar abusos, las EPO solo deben ser validadas por las autoridades competentes si existen razones apremiantes que den lugar a un grado suficiente de sospecha para justificar la confiscación transfronteriza de datos.**

[1] Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE

[2] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas

4. Mecanismo efectivo para garantizar la aprobación

Para que las reglas de aprobación sean efectivas, existe la necesidad, cuando corresponda, de que haya 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 responsable de datos (en línea con las observaciones anteriores). Se agradece que esto no siempre sea apropiado, especialmente cuando existe un riesgo de destrucción de la prueba. **En tales casos, se debe considerar la posibilidad de establecer un proceso en dos etapas en el que se pueda utilizar una Orden Europea de Conservación para asegurar la prueba antes de cualquier solicitud impugnada de una Orden de Entrega.**

5. Motivos de denegación de ejecución

CCBE considera que los motivos de denegación para ejecutar una EPO establecidos en el Artículo 9 (5) son demasiado restrictivos. Además de razones técnicas o prácticas (por ejemplo, el Certificado EPO (EPOC) está incompleto o el destinatario no puede cumplir debido a *fuerza mayor*), el único motivo sustantivo de no ejecución que puede invocar el destinatario es que si considera que "basado con 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". **Debería haber motivos más amplios para rechazar la ejecución de una EPO, incluida la ausencia de doble incriminación o, como se señaló anteriormente, 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/privilegio profesional legal es per se una violación del derecho a un juicio justo de conformidad con el artículo 6 del CEDH y, como tal, debe reconocerse como un motivo único y suficiente para denegar la ejecución de una EPO.**

6. Notificación del sujeto de los datos

El artículo 11(2) especifica que la persona cuyos datos se buscan debe ser informada "sin demora indebida sobre la entrega de datos". Sin embargo, esto "puede demorarse el tiempo que sea necesario y proporcionado para evitar la obstrucción del proceso penal". Por lo tanto, las autoridades pueden ignorar fácilmente los requisitos de notificación, ya que siempre hay un motivo para descubrir por qué podría poner en peligro la investigación.

Esto socava severamente los derechos de las personas a un juicio justo porque, mientras no sepan que se han tomado sus datos, no pueden hacer valer sus derechos. **Por lo tanto, la imposición de restricciones de confidencialidad a las EPO debe estar sujeta a la aprobación de una autoridad judicial independiente y, en cada caso, estar debidamente motivada y justificada por la autoridad emisora sobre la base de evaluaciones significativas y documentadas.**

7. Los derechos de la defensa

Cualquier propuesta para la recuperación de pruebas electrónicas no debe considerarse como un asunto exclusivo del enjuiciamiento. Los derechos de defensa deben tener la debida consideración. La propuesta no tiene debidamente en cuenta el requisito de igualdad de medios en los procedimientos penales, que es un concepto reconocido por el Tribunal Europeo de Derechos

Humanos 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 una prueba electrónica.

Por tanto, CCBE considera que, al igual que con la 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 lo hacen los fiscales. De lo contrario, la propuesta socava el principio de la igualdad de medios entre la acusación y la defensa, lo que coloca al acusado en una situación de desventaja.

Además, la propuesta no proporciona ningún requisito u orientación a los destinatarios para limitar la transmisión de la prueba electrónica a los datos que son relevantes para los fines de la investigación criminal. Como resultado, las LEA podrían verse abrumadas con los datos. Tampoco hay ninguna disposición para garantizar que los demandados no se sobrecarguen por el peso de la prueba electrónica, o que dicha prueba electrónica obtenga los metadatos apropiados, como un índice y una tabla de contenidos. Sin la ayuda de tales metadatos, es muy difícil o incluso imposible para los abogados afirmar efectivamente los derechos de sus clientes.

8. Revisión judicial

Debería considerarse la posibilidad de disponer de un medio judicial efectivo análogo al mecanismo previsto en el artículo 42 del Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea, en particular en relación con la competencia del Tribunal de Justicia de conformidad con el artículo 267 del Tratado de Funcionamiento de la Unión Europea.