

## Respuesta de CCBE a la consulta pública sobre el acceso transfronterizo a las pruebas electrónicas en materia penal.

20/10/2017

El Consejo de la Abogacía Europea (CCBE), representa a las abogacías de 45 países, y a través de ellos representan a más de un millón de abogados europeos. CCBE responde regularmente a través de sus miembros sobre asuntos que afectan a los ciudadanos Europeos y abogados.

En este documento, CCBE responde a la [consulta pública](#) presentada por la Comisión sobre el acceso transfronterizo de las pruebas electrónicas en materia penal. CCBE considera de gran importancia esta consulta, sin embargo, el cuestionario, que principalmente se dirige a las autoridades públicas y los distribuidores de servicios IT, está estructurado de manera que no se obtiene respuesta relacionada con el área de preocupación de CCBE. En este documento, se responde al cuestionario y se hace unas observaciones generales sobre posibles iniciativas de la UE en pruebas electrónicas

En abril de 2014, CCBE publicó su [estudio comparativo sobre vigilancia gubernamental de los datos de los abogados en la nube](#). En este documento CCBE expresó sus preocupaciones sobre divergencia entre las reglas normales de búsqueda y la incautación de la prueba o incluso la inexistencia virtualmente de normas relativas al acceso de la prueba digital o interceptación de transmisión de datos.

Esta incertidumbre regulatoria llega a ser peligrosa cuando los datos y las comunicaciones a los que acceden las autoridades son aquellos a los que la ley les ha otorgado especial protección. Esto es el caso claro en relación con las comunicaciones entre los abogados y sus clientes. En todos los Estados miembros de la UE, el derecho protege la divulgación de la información comunicada confidencialmente entre el abogado y el cliente. Este principio – generalmente referido como secreto profesional o privilegio profesional – ha sido reconocido por la mayor parte de jurisdicciones desde hace siglos, y también por el Tribunal de Justicia de la UE en el caso AM&S ([C-155/79](#)).

La protección del secreto o confidencialidad de los datos o la posesión de los abogados es una fundación del Estado de derecho. Los regímenes reglamentarios desarrollados independientemente por todas las jurisdicciones a través de la UE refleja esa norma fundamental en sus respectivas normas aplicadas para las búsquedas e incautaciones de la pruebas en los locales de abogados.

Sin embargo, las normas no siempre se han mantenido al ritmo de la tecnología cambiante. Por tanto, en algunas jurisdicciones, el formulario electrónico que se conserva en las instalaciones de un proveedor de IT en nombre de un abogado, goza de menos protección que esos datos almacenados en la propia oficina del abogado. CCBE no ve justificación para tal distinción.

Si la sociedad considera que esos datos requieren protección, no puede haber una justificación adecuada para tal diferenciación. En el entorno moderno de IT, esa diferenciación tampoco es natural: las personas que usan la misma interfaz de usuario para acceder, compartir, comunicar o almacenar datos, no pueden reconocer si la información proviene de un ordenador u otro. La misma regla sigue el abogado que utiliza el ordenador si los datos electrónicos del cliente se enviaron como un archivo adjunto de correo electrónico o simplemente se compartieron con el destinatario después de la identificación de este último.

Otra área de incertidumbre regulatoria surge debido a la circunstancia de que, en algunos países, por la forma en la que está redactada la protección de la información de los abogados, no está claro si las disposiciones relevantes se aplican sobre la información almacenada en los proveedores de servicios externos.

Tales circunstancias podrían alentar a las autoridades policiales a dirigirse directamente al proveedor de servicios en la nube para obtener información almacenada en su servidor o servidores (sin orden judicial en algunos países), en lugar de ir a las instalaciones del abogado con la orden apropiada emitida por la autoridad judicial.

Estos problemas se agrava con que no hay una buena manera técnica para que tanto el proveedor de servicios en la nube como hosting o un externo (como una agencia o poder estatal) puedan identificar material protegido por el privilegio legal o secreto profesional.

A la vista de todas las ambigüedades existentes a nivel nacional, lo más importante es que cada iniciativa de la UE que regula el acceso transfronterizo de las pruebas digitales establezca salvaguardas para proteger los derechos fundamentales.

CCBE hace una llamada a las instituciones de la UE para adherir los siguientes principios:

- A. El principio principal debe ser que cualquier protección que se conceda en el mundo del papel también debe otorgarse en el mundo electrónico.

Los mismos principios se deben aplicar a los datos en un contexto digital, como es el caso de los datos que se almacenan físicamente en las instalaciones de una persona o de una organización. En el caso de los abogados, esto significa que, en la medida en que las reglas relativas al mundo físico de la oficina de un abogado prevén, por ejemplo, la presencia de representantes del colegio de abogados en los registros de su despacho, debe adoptarse una disposición análoga para búsquedas virtuales (transfronterizas). En otras palabras, el uso de servicios de comunicaciones electrónicas u otros servicios en la nube por parte de los abogados debe protegerse de la misma manera independientemente de si el contenido se almacena en un centro de datos o en un ordenador en la oficina del abogado o de su persona. Esto puede implicar una mayor estandarización del trabajo IT, incluyendo los proveedores de servicios en la nube, pero CCBE considera que se debe de hacer.

- B. Regulación efectiva no debe ser razonablemente capaz de ser eludida. No debemos volver por defecto a una protección mínima.

Debe garantizarse que cuando exista un régimen estricto en vigor para proteger los datos de los abogados, las autoridades pertinentes no pueden eludir ese régimen haciendo solicitudes de datos transfronterizas formales o informales directamente a los abogados de los proveedores de servicios IT para producir información. Cuando se aplica una orden de búsqueda, se debe notificar a una organización, permitiendo evaluar sus derechos y obligaciones legales, y si es posible, se debe poder impugnar la solicitud antes de que se pueda incautar cualquier información. Esto implica que las solicitudes de acceso a la evidencia digital deben, siempre que sea posible, dirigirse siempre a los controladores de datos, en lugar de a los procesadores de datos.

- C. Cualquiera que sea el régimen establecido para el acceso transfronterizo a la evidencia digital, ese régimen debe garantizar la inviolabilidad de los datos y otras pruebas que entren en el ámbito del principio de privilegio profesional o secreto profesional.

Todas las protecciones establecidas para las búsquedas e incautaciones deberían aplicarse también si los datos son interceptados de manera transfronteriza y que se acceda a ello durante el transcurso, como parte de una comunicación, no importa si la entidad que realiza técnicamente la interceptación es un proveedor de proveedor de servicios de comunicación electrónica, un proveedor de servicios IT o una agencia de gobierno actuando directamente. El contenido que contiene el secreto profesional o información legal privilegiada, y que es procesada por un servicio de comunicación electrónica o un proveedor de servicios en nube (incluyendo un proveedor de servicio de correo), no debería ser accesible para agencias del gobierno.

Para este fin, las fuerzas del orden deberían estar obligadas a utilizar todos los medios tecnológicos que disponibles para asegurarse que todo lo que compete al secreto profesional queda fuera del alcance de las operaciones de vigilancia. Una solución realista consistiría en requerir a los servicios de comunicación electrónica y los proveedores de servicios en nube a ofrecer a los abogados una opción para indicar tal información, evidentemente, solo tras una verificación clara de que el usuario de verdad necesita el abogado que ha solicitado. Por ejemplo, en los Países Bajos, existe un sistema de verificación número de teléfono que es capaz de reconocer los números de teléfono de los abogados y parar la vigilancia.

#### Respuestas de CCBE al [cuestionario](#):

En la lista que se presenta seguidamente, solo se han copiado aquellas preguntas que se consideran relevantes para CCBE. La respuesta del resto de preguntas no incluidas en la lista no tiene opinión.

#### Parte II: Preguntas generales y situación actual en tu país/entidad

**\*26 ¿Debería la Comisión Europea proponer medidas para mejorar la cooperación directa de las fuerzas del orden y autoridades judiciales de la UE con la sede central de los proveedores de servicios digitales en terceros países bajo la condición de que hay suficientes salvaguardas para proteger tus derechos fundamentales?**

- Si
- No

No hay opinión

27 ¿Cuáles son los problemas que podrían plantear una iniciativa de la UE en el campo de las pruebas electrónicas?

	Muy relevante	Relevante	Un poco relevante	No relevante	Sin opinión
* Impacto negativo (fundamental) en los derechos garantizados por el derecho nacional/ derecho UE	X	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
* Pérdida de soberanía para tu Estado miembro	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X
* Riesgo de que terceros países impongan obligaciones para los proveedores de servicios para divulgar pruebas electrónicas almacenadas en la UE (reciprocidad)	X	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

28 ¿Cuáles son los problemas que podrían plantear una iniciativa de la UE en el campo de las pruebas electrónicas?

	Muy relevante	Relevante	Un poco relevante	No relevante	Sin opinión
* Menos competencias en comparación con la situación actual	0	0	0	0	X
* Confusión de los instrumentos (EIO, Convención Budapest, MLA)	X	0	0	0	0
* Dificultades para ejecutar la solicitud	0	X	0	0	0

29 ¿Cuáles son los problemas que podrían plantear una iniciativa de la UE en el campo de las pruebas electrónicas?

	Muy relevante	Relevante	Un poco relevante	No relevante	Sin opinión
*Naturaleza obligatorio	0	0	0	0	X
*Incrementando el volumen de solicitudes	0	0	0	0	X
* Impedir la confianza del cliente en sus servicios	X	0	0	0	0

33. ¿Qué esperas que se consiga con la iniciativa de la UE sobre pruebas electrónicas?

	Si	No	No hay opinión
*Certeza legal	X	0	0
*Garantía de protección sobre los derechos fundamentales en concordancia con la carta de derechos fundamentales,	X	0	0

35. ¿Además de la posibilidad de establecer un marco legal para los casos transfronterizos, crees que esta iniciativa de la UE podría también cubrir casos puramente domésticos?

- Si
- No
- No hay opinión

### Parte III. Acceso a pruebas electrónicas por una solicitud directa de un proveedor de servicios digitales

**58 Una posible iniciativa de la UE podría autorizar a las autoridades policiales a solicitar directamente (a través de un “requerimiento de producción”) u obligar (orden producción) a un proveedor de servicios en otro Estado miembro a divulgar información específica sobre un usuario sin haber acudido a las autoridades policiales o judiciales en otro Estado miembro. Crees que la iniciativa de la UE debería cubrir**

	Si	No	No hay opinión
*Una solicitud directa al proveedor de servicios (medida voluntaria)	0	0	X
*Una orden directa al proveedor de servicios (medida obligatoria)	0	X	0

**59 Si la Comisión Europea propone un marco legal para las solicitudes directas transfronterizas a los proveedores de servicios: ¿Cómo de relevante son las siguientes condiciones para un posible instrumento transfronterizo para el acceso a las pruebas electrónicas (Por favor puntúe la relevancia abajo)?**

	Muy relevante	Relevante	Un poco relevante	No relevante	Sin opinión
*El acceso directo debería solo ser dado para un número limitado de delitos (Ejemplo dependiendo de la gravedad)	X	0	0	0	0
* La condición de que el acto sea punible en los dos países (doble penalidad)	X	0	0	0	0
*Salvaguardas específicas para asegurar los derechos fundamentales	X	0	0	0	0
*La notificación a otro Estado miembro que se vea afectado por la medida.	X	0	0	0	0
*Posibilidad por el Estado miembro al que se le ha notificado de oponerse a la medida.	X	0	0	0	0
*Notificación de la persona en cuestión	X	0	0	0	0
*Remedios legales para la persona afectada.	X	0	0	0	0

**Parte IV. Acceso directo a pruebas electrónicas a través de un sistema de información sin ningún intermediario (Ej. un proveedor de servicios) de por medio.**

Podría darse la situación por ejemplo, un registro en las dependencias de un sospechoso donde se busque o se acceda a la información que tiene almacenada de forma electrónica directamente de confiscar el dispositivo, pero podría ser impreciso donde son almacenados los datos o si hay dimensión transfronteriza.

**\*64 ¿Ve alguna necesidad de un marco legal europeo para esta situación?**

- Si

No

No hay opinión

**\* Si la Comisión Europea decidiera proponer un marco legal para esta situación, que debería proporcionar la propuesta?**

	Si	No	No hay opinión
*La condición de que el acto sea punible en los dos países (doble penalidad)	X	0	0
* Salvaguardas específicas para asegurar los derechos fundamentales	X	0	0
* La notificación a otro Estado miembro que se vea afectado por la medida.	X	0	0
*Posibilidad por el Estado miembro al que se le ha notificado de oponerse a la medida.	X	0	0
*Notificación de la persona en cuestión	X	0	0
*Remedios legales para la persona afectada.	X	0	0