Capítulo 9

Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo[1]

Montserrat de Hoyos Sancho

Catedrática de Derecho Procesal
Ex–Directora del Instituto de Estudios Europeos
Universidad de Valladolid

I. IMPORTANCIA DE LA OBTENCIÓN TRANSFRONTERIZA DE INFORMACIÓN ELECTRÓNICA DE LA QUE DISPONEN LOS PROVEEDORES DE SERVICIOS ON-LINE E INSUFICIENCIA DE LA NORMATIVA ACTUAL EN LA UNIÓN EUROPEA

Pocas dudas podemos albergar acerca de la importancia que la llamada "prueba electrónica" o *e-evidence* tiene y seguirá teniendo en la investigación y enjuiciamiento de hechos delictivos.

La necesidad de recabar información electrónica, y en concreto aquella de la que disponen los que genéricamente conocemos como "proveedores de servicios de internet", es algo con lo que los operadores jurídicos tienen que contar, según los últimos datos publicados[2], en un 85% de las investigaciones penales, incluso aunque el delito no se hubiera cometido

1. Este trabajo es resultado del Proyecto de investigación del Ministerio de Ciencia e Innovación: *"Proceso penal y Unión Europea. Análisis y propuestas"* –PID2020-116848GB-100–, así como del Grupo de Investigación Reconocido "*Garantías procesales y Unión Europea*", de la Universidad de Valladolid.

2. *Vid*. más ampliamente los datos contenidos en el documento de la Comisión europea *Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border*

a través de medios informáticos. Así, para investigar y probar *v.gr.* un simple homicidio con arma blanca, puede ser necesario obtener pruebas digitales del tipo: correos electrónicos entre autor y víctima, consulta de sus perfiles privados de Facebook o Instragram, mensajes de WhatsApp, compras online, coordinadas de GPS de una ruta determinada, rastreo de información buscada en internet, etc. Además, esas mismas fuentes nos indican que en dos tercios de estas investigaciones tales pruebas tuvieron que obtenerse de proveedores de servicios *on line* implantados en territorios de otras jurisdicciones.

Por lo tanto, está claro que es imprescindible disponer de instrumentos normativos que permitan a las autoridades competentes obtener esa información electrónica tan necesaria, de manera selectiva, rápida y fiable, al tiempo que se asegura el pleno respeto de los derechos esenciales, que desde luego incluyen las garantías procesales fundamentales, así como la protección de la información y los datos personales.

En el ámbito jurídico de la Unión Europea ya disponemos desde hace años de una valiosa herramienta para la obtención transfronteriza de pruebas: la orden europea de investigación[3] –OEI en lo sucesivo–. Pero este que ha demostrado ser un instrumento de cooperación muy eficaz, basado en la comunicación directa entre autoridades y en el reconocimiento mutuo de resoluciones judiciales, presenta limitaciones importantes cuando lo que se necesitan son pruebas electrónicas o digitales que están en poder de los proveedores de servicios de internet, en sentido amplio.

En muchos casos tales proveedores estarán radicados en países distintos de aquellos en los que se tramita la investigación o la causa penal, por lo que será preciso acudir a la cooperación transfronteriza[4]. Sin embargo, incluso tratándose de países entre los que está vigente el sistema de la OEI, éste puede ser un instrumento insuficiente, por las siguientes razones: es muy probable que los datos electrónicos que se necesitan estén dispersos

access to electronic evidence for judicial cooperation in criminal matters, COM (2019) 70 final, pp. 1 y ss., publicada en Bruselas el 5.2.2019.

3. Directiva 2014/41/CE del Parlamento europeo y del Consejo, de 3 de abril de 2015, relativa a la orden europea de investigación en materia penal, DOUE 1.5.2014, L. 130/1. Transpuesta al ordenamiento español por Ley 3/2018, de 11 de junio, incorporando el instrumento OEI en el Título X de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, BOE núm. 282, de 21.11.2014.

4. Si el proveedor de servicios que ha de proporcionar los datos electrónicos que se necesitan en una causa penal estuviera establecido en el mismo Estado en que se investigan o enjuician los hechos, no sería necesaria la cooperación transfronteriza para su obtención; se trataría entonces de una prueba "doméstica".

en servidores de distintos Estados, también fuera de la UE, puede que ni siquiera se sepa en qué países están en el momento en que se ha de cursar la petición, o incluso que estén repartidos en servidores de distintos países, o que la información electrónica esté almacenada de manera itinerante. Tengamos presente que los servicios basados en el uso de internet se pueden prestar desde cualquier lugar, pues no requieren infraestructura o personal en el país donde en efecto se ofrece y se presta el servicio.

De otro lado, los datos electrónicos son extremadamente "volátiles", de tal manera que la tramitación de una OEI[5], por rápida que fuera, podría resultar demasiado lenta[6], y perderse esa prueba en el lapso de tiempo que fuera necesario emplear para su solicitud[7].

Por estas razones, expuestas ahora de manera sucinta, el legislador de la Unión ha considerado que para la obtención de este tipo de pruebas o datos electrónicos era necesario designar como destinatario de la solicitud de cooperación directamente al *prestador de servicios on line* que está establecido, representado o que presta sus servicios en la Unión, en un Estado distinto de aquél en que se sigue la investigación o el proceso penal, no siendo por tanto relevante a estos efectos el concreto lugar o lugares donde pudieran estar almacenadas la información electrónica, ni dónde tenga su sede central o delegaciones la compañía que presta el servicio.

El principio de territorialidad en relación con la concreta ubicación o almacenamiento de los datos, que según el sistema OEI determinaría el país/autoridad a la que debe remitirse la Orden con la solicitud de cooperación, deja por tanto de ser operativo cuando hablamos de este tipo de pruebas almacenadas "en la nube"[8].

---

5. En la Directiva OEI se hace mención expresa a la posible obtención de información transfronteriza sobre titulares de un número de teléfono o de una dirección IP concreta, y no se descarta que se pueda emplear para la obtención de otro tipo de datos electrónicos almacenados por los proveedores de servicios que fueran necesarios para la investigación y prueba de hechos delictivos. *Vid.* art. 10.1.e).
6. Así lo destaca BUENO DE MATA, F.: "Análisis de las medidas de cooperación judicial internacional para la obtención transfronteriza de pruebas en materia de cibercrimen", en *La transformación digital de la cooperación jurídica penal internacional.* L. Fontestad (Dir.), Cizur Menor: Aranzadi, 2021, esp. p. 27.
7. En el sistema OEI está previsto que, salvo en casos graves o urgentes, la autoridad de ejecución deberá adoptar la resolución de reconocimiento o ejecución "a más tardar en 30 días después de la recepción de la OEI", y deberá llevar a cabo tal medida de investigación sin demora "a más tardar 90 días después". *Vid*. art. 12 Directiva OEI.
8. Sobre la necesidad de dejar de lado el principio de territorialidad en este materia, entre otros: TOSZA, S.: "All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order", *New Journal of European Criminal Law*, vol. II (2), 2020, pp. 161 y ss., esp. p. 170; TINOCO PASTRANA, A.: "Las órdenes europeas de entrega

II. LA PROPUESTA DE REGLAMENTO DE LA UNIÓN EUROPEA SOBRE ÓRDENES EUROPEAS DE ENTREGA Y CONSERVACIÓN DE PRUEBAS ELECTRÓNICAS A EFECTOS DEL ENJUICIAMIENTO PENAL

Tratando de dar respuesta a las necesidades apuntadas en las líneas precedentes, las instituciones UE debaten actualmente sobre este texto presentado el 14 de abril de 2018 por la Comisión europea: *Propuesta de Reglamento del Parlamento europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal*[9], que no sustituirá a la ya vigente OEI, sino que ambas herramientas coexistirán; se empleará una u otra en función de las necesidades de la causa concreta.

Este Reglamento[10] y la Directiva que le acompaña[11] obligarán a todos los proveedores de servicios online que operen en la Unión a designar representantes legales para dar respuesta a las solicitudes de cooperación

---

y conservación: la futura obtención transnacional de la prueba electrónica en los procesos penales en la Unión Europea", *Cuadernos de política criminal*, núm. 135, 2021, pp. 203 y ss.; LARO GONZÁLEZ, E.: "El Reglamento E-evidence: instrumento adicional a la Orden europea de investigación", *La Ley Probática*, núm. 3, 2021, pp. 1 y ss., esp. p. 6.

9. Documento COM (2018), 225 final. Pueden verse sobre esta Propuesta los comentarios y valoraciones de FUENTES SORIANO, O.: "Europa ante el reto de la prueba digital. El establecimiento de instrumentos probatorios comunes: las órdenes europeas de entrega y conservación de pruebas electrónicas", en *Era digital, sociedad y derecho.* O. Fuentes Soriano (Dir.), Valencia: Tirant lo Blanch, 2020, pp. 281 y ss., el *supra* citado trabajo de TINOCO PASTRANA, así como BUJOSA VADELL, L.: "Cooperación judicial para la obtención y transmisión de pruebas electrónicas", en *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, L. Fontestad (Dir.), Cizur Menor: Aranzadi, 2022, pp. 79 y ss., y BUENO DE MATA, F.: "Análisis de las medidas…", *op. cit.*, pp. 19 y ss. Más recientemente me he ocupado específicamente del tema en DE HOYOS SANCHO, M.: "Reflexiones acerca de la propuesta de Reglamento UE sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos del enjuiciamiento penal", *RGDP,* núm. 58, 2022, pp. 1 y ss.

10. Como apuntan GIALUZ y DELLA TORRE, el uso del instrumento normativo "Reglamento" es una buena prueba de que la Unión se fía realmente poco de cómo los Estados miembros reciben habitualmente los instrumentos eurounitarios en materia procesal penal, por lo que en este caso han optado por eludir el problema, proponiendo un acto *self-executing*. *Vid.* su trabajo "Lotta alla criminalità nel cyberspazio: la Commisione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali", *Diritto Penale Contemporaneo*, núm. 5, 2018, pp. 277 y ss., esp. p. 292.

11. Junto a este documento, el 17 de abril de 2018 se presentó también una propuesta de Directiva del Parlamento europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales, COM (2018) 226 final.

y suministrar los datos requeridos, a no ser que concurra alguna de las muy limitadas causas de denegación expresamente previstas en la norma.

Resumiremos a continuación los elementos definidores de este nuevo instrumento de cooperación transfronteriza, tal y como fue diseñado por la Comisión en la citada Propuesta.

Según disponen los arts. 1 y 3, el Reglamento será de aplicación a los supuestos en que una autoridad competente de un Estado miembro UE[12] necesite obtener datos almacenados por un proveedor de servicios de pago que esté establecido, representado, u ofrezca servicios[13] en el territorio de otro Estado miembro, con independencia de la ubicación de los datos, siempre que éstos sean necesarios como elementos de investigación o prueba en procesos penales concretos.

Estas decisiones "vinculantes y obligatorias" que emitan las autoridades competentes, las órdenes de conservación y entrega de pruebas electrónicas, sólo podrán remitirse con este carácter transfronterizo si a nivel nacional, en el propio Estado emisor de las mismas, existe la posibilidad de adoptar una medida similar para la misma infracción y en una situación comparable. Se pretende así evitar el *forum shopping*, es decir, que se soliciten fuera del país medias que no podrían adoptarse en el propio ordenamiento. Además, no podrán tener una finalidad meramente prospectiva o preventiva; los hechos que se investigan habrán de ser delitos concretos, ya cometidos y en relación con autores específicos, y los datos que se piden son datos almacenados por el proveedor en el momento de cursar la petición, no los que pudieran obtenerse en el futuro, tras la recepción de la orden.

La norma proyectada parte de una distinción generalmente admitida entre dos categorías de datos almacenados que podrían solicitar y obtener las autoridades competentes –*Vid.* art. 2–. Por un lado, los datos no relativos al contenido, entre los que se contarían los datos de los abonados[14],

12. En los Considerandos 64.º y 65.º podemos leer que Irlanda ha notificado su deseo de participar en la adopción y aplicación de este Reglamento, mientras que Dinamarca no lo hará.

13. El proveedor de servicios ha de tener una "vinculación significativa" con uno más Estados miembros. Si no tuviera establecimiento como tal, bastará con que tenga un número significativo de usuarios, e incluso podrá deducirse su vínculo con Estados UE considerando otros factores, como la lengua o la moneda empleada en su oferta de productos, publicidad local de sus servicios, o la disponibilidad de una aplicación móvil en esos Estados miembros. *Vid.* más ampliamente, Exposición de motivos de la Propuesta, p. 16.

14. Son datos de los abonados cualquier dato en relación con su identidad: nombre, fecha de nacimiento, dirección postal, datos sobre facturación y pagos, teléfono, dirección de email, tipo de servicio y duración, incluidos otros datos técnicos, como los de interfaces, de validación de uso del servicio, etc. *Vid.* art. 2, apdo. 6.º.

los de acceso[15] y los de transacciones[16]; por otro lado, con un tratamiento diferenciado, estarían los datos de contenido[17]. La entrega o conservación de cada uno de esos tipos de datos conlleva distintos grados de injerencia en los derechos del afectado, por lo que en el texto se establecen condiciones y garantías diferentes para cada supuesto –*Vid.* arts. 4 y ss.–.

En todo caso, una orden de estas características solo podrá emitirse si fuera necesaria y proporcionada en el caso concreto para alcanzar un fin legítimo, como es la obtención de datos relevantes y necesarios para la investigación y prueba de hechos concretos.

Las órdenes de entrega de datos de abonados o de acceso podrán emitirse, para la investigación de todo tipo de delitos, por un juez, por un fiscal o incluso por la policía, con validación posterior en el último caso. Para la petición de entrega de datos de transacciones o de contenidos, ha de tratarse de delitos que conlleven más de tres años de privación de libertad, o que afecten a un gran número de personas o de terrorismo, y solo un juez podrá emitir esas órdenes.

Las órdenes de conservación de información electrónica pueden emitirse por juez o fiscal competente, o incluso por la policía, sea cual fuere el tipo y gravedad de la infracción penal, pues su finalidad es evitar la eliminación o modificación de datos, para preparar posteriormente una orden de entrega o una OEI.

Las referidas órdenes de entrega o conservación se remitirán directamente al representante legal designado por el proveedor de servicios, indica la Propuesta de Reglamento en su art. 7, aunque lo que realmente se remitirá será un "Certificado" –no la orden propiamente dicha, en la que sí constarán todos los datos de la causa, la motivación de la orden, la justificación de la necesidad y proporcionalidad de la medida, etc.–. Esos "Certificados" son documentos multilingües y estandarizados, en

15. Son datos relativos al acceso aquellos que se refieren al inicio y final de una sesión del servicio, fecha y hora de acceso o conexión y desconexión, dirección IP asignada al usuario por el proveedor de servicios de internet, datos de la interfaz utilizada y de identificación del usuario; incluye los metadatos de comunicaciones electrónicas. *Vid.* art. 2, apdo. 7.º.

16. Son datos de transacciones relacionadas con la prestación de un servicio por ese proveedor que facilitan información contextual o adicional sobre ese servicio, como origen y destino de un mensaje, ubicación del dispositivo, fecha, hora, duración, tamaño, ruta, formato y protocolo utilizado, tipo de compresión, siempre que éstos no sean datos relativos al acceso. También se incluyen aquí los metadatos. *Vid.* art. 2, apdo. 8.º.

17. Datos de contenido son aquellos almacenados en formato digital, como textos, voz, videos, imágenes o sonidos, distintos de los datos de los abonados, de acceso o transacciones. *Vid.* art. 2, apdo. 9.º.

los que evita el uso de "texto libre" para reducir el coste de traducción todo lo posible; se denominan respectivamente EPOC y EPOC-PR[18], por sus siglas en inglés, y se transmitirán por cualquier medio que garantice su autenticidad, indica el art. 8.

Los plazos previstos para dar cumplimiento al EPOC recibido, dando respuesta directa a la autoridad emisora, son los siguientes: a más tardar en 10 días desde la recepción, salvo que se solicitara una actuación más rápida; en casos urgentes puede solicitarse que se remitan "sin demora, a más tardare en un plazo de seis horas tras la recepción" –*Vid.* art. 9, apdo. 2.º–. Si el destinatario de la orden, el proveedor de servicios, no pudiera cumplirla, podría pedir información adicional a la autoridad de emisión y, en último término, informar a ésta de que no podrá satisfacer la solicitud recibida.

Para el cumplimiento de un EPOC-PR el art. 10 dispone que el proveedor de servicios deberá conservar sin demora los datos solicitados, y tal preservación expirará tras 60 días si no se ha puesto en marcha antes la petición de entrega[19].

Por lo demás, la persona cuyos datos se han solicitado sólo será informada de la emisión y cumplimiento de estas órdenes posteriormente, una vez transcurrido el tiempo "necesario y proporcionado" para que no se vea afectado el proceso penal en curso. Esa información posterior al usuario del servicio por parte de la autoridad de emisión incluirá la relativa a las vías de recurso disponibles –*Vid.* arts. 11 y 17–.

Una cuestión que a nuestro juicio afectará notablemente a la eficacia práctica que finalmente puedan alcanzar estas órdenes de entrega y conservación es la relativa a las posibles sanciones en caso de incumplimiento, y la subsidiaria intervención en esos casos de la autoridad del Estado de ejecución.

La Propuesta de Reglamento prevé que, sin perjuicio de posibles sanciones penales previstas en las leyes nacionales, los Estados miembros

18. Los modelos de certificados se encuentran en los Anexos I y II de la propuesta de Reglamento.

19. En el sistema de la OEI pueden alcanzar los 30 días para la decisión de reconocimiento, prorrogables por otros 30, y hasta 90 días más para la ejecución, ampliables otros 30, véase el art. 12 de la Directiva OEI. *Vid.* también el análisis contenido en ARANGÜENA FANEGO, C.: "Orden europea de investigación: próxima implementación en España del nuevo instrumento de obtención de prueba penal transfronteriza", *Revista de Derecho Comunitario Europeo,* núm. 58, 2017, pp. 905 y ss., esp. pp. 932 a 934; LARO GONZÁLEZ, E.: *La Orden Europea de Investigación en el espacio europeo de justicia,* Valencia, 2021, pp. 217 a 224; LLORENTE SÁNCHEZ-ARJONA, M.: *La orden europea de investigación y su incorporación al ordenamiento español*, Valencia: Tirant lo Blanch, 2020, pp. 159 a 162.

deberán establecer sanciones pecuniarias en caso de que los proveedores de servicios incumplan con sus obligaciones de entrega o conservación de datos requeridos, que deberán ser "eficaces, proporcionadas y disuasorias"; nada más se indica al respecto en el art. 13.

Además, si el proveedor no cumpliera en plazo la orden recibida, ni aportara razones aceptadas por la autoridad emisora, ésta podrá trasladar su petición a la autoridad competente del Estado de ejecución, para que tome las medidas de coerción necesarias en un máximo de 5 días, a no ser que concurran motivos de rechazo.

Por lo que respecta a los motivos de oposición a la ejecución de las órdenes que puede esgrimir el destinatario de las mismas, es decir, el proveedor de servicios, el art. 14 de la Propuesta enuncia los siguientes, que son de carácter facultativo[20]: la orden no fue emitida o validada por autoridad competente, o no se refiere a alguna de las infracciones admitidas, o es imposible cumplirla por razones materiales o de fuerza mayor, o por errores en el certificado no subsanados, o porque el proveedor afirma no disponer de esos datos, o por no estar cubierta la solicitud por el Reglamento. Se añade también como motivo genérico de oposición a la ejecución de la orden que ésta sea contraria a la Carta de Derechos Fundamentales de la UE o manifiestamente abusiva[21].

Es sin duda destacable que este listado de motivos de rechazo no incluya una referencia al incumplimiento del requisito de doble incriminación, por lo que sería posible tener que ejecutar una orden para investigar o enjuiciar hechos delictivos en el Estado de emisión, que no lo son en el de ejecución. A nuestro juicio, en este punto se debería haber seguido el criterio tradicional de exención de la exigencia de doble incriminación para el listado de los 32 "eurodelitos", por encima del umbral punitivo de los tres años[22].

Por lo que respecta a las vías de impugnación de que disponen las personas investigadas o acusadas cuyos datos se hayan obtenido a través de

20. Llamamos la atención sobre el carácter facultativo de esta oposición por parte del proveedor de servicios, pues el precepto dice "podrá", y no "deberá" o "tendrá que". A nuestro juicio, este precepto tendría que estar redactado en sentido imperativo, de tal forma que, si en efecto concurrieran los motivos de oposición, el proveedor de servicios estaría obligado a responder a la autoridad emisora oponiéndose al cumplimiento de la orden recibida.

21. Recordemos en este punto que la información de que dispone la autoridad de ejecución es muy sucinta, solo la contenida en el Certificado EPOC o EPOC-PR.

22. En la OEI este sí es un motivo de denegación de la ejecución, de carácter facultativo. Más ampliamente sobre esta cuestión, DE HOYOS SANCHO, M.: "La Orden Europea de Investigación: reflexiones sobre su potencial efectividad a la vista de los motivos de denegación del reconocimiento y ejecución en España", *Revista General de Derecho Procesal,* núm. 47, 2019, pp. 1 y ss., esp. pp. 16-18.

órdenes de entrega, el art. 17 de la Propuesta dispone que éstas deberán ser "vías de recurso efectivas", que podrán emplearse "durante el proceso penal para el que se haya emitido esa orden". Por tanto, los recursos se ejercitarán en el Estado emisor de las órdenes, lo que puede complicar el ejercicio del derecho de defensa de los afectados por éstas cuando sean residentes en el Estado de ejecución.

En último término y a modo de resumen, las principales objeciones de fondo planteadas a esta Propuesta de Reglamento, documento que ha suscitado un intenso debate en diversos ámbitos jurídicos[23], son las siguientes:

¿Estamos realmente ante un instrumento de reconocimiento mutuo en sentido estricto? La respuesta ha de ser negativa a nuestro juicio, pues tal principio rector de la cooperación transfronteriza en el ámbito UE, al menos como ha venido siendo entendido hasta hoy, implica un doble control, por la autoridad de emisión y también por la de ejecución, el cual no existe en esta Propuesta de Reglamento, pues se trata de un sistema de cooperación directa con el proveedor de servicios, quien en la gran mayoría de los casos ejecutará sin un control judicial previo las órdenes que reciba. Según se ha expuesto, la autoridad del Estado de ejecución sólo intervendrá de manera excepcional, si el proveedor se niega a cumplir con el Certificado recibido.

De otro lado, este modelo de cooperación directa con los proveedores de servicios implica una "privatización" de la confianza mutua[24] y de la

23. Más allá del ámbito estrictamente académico, *Vid.* entre otros los informes de FAIR TRIALS de los años 2018 y 2019, respectivamente: "Position Paper: The new proposed EU Production and Preservation Orders", "Consultation Paper: E-evidence Position Paper", o del COUNCIL OF BARS AND LAW SOCIETIES OF EUROPE –CCBE–: *Posición del CCBE sobre la Propuesta de Reglamento de la Comisión sobre las Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos del enjuiciamiento penal*, de 19 de octubre de 2018. Muy valioso también el informe coordinado por CARRERA, STEFAN y MITSILEGAS, presentado en octubre 2020 por el CEPS-QMUL *Task Force*, Centre for European Policy y Queen Mary University of London, *Cross-border data access in criminal proceedings and the future of digital justice. Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic*.

24. Críticos con la aplicación de este principio a la obtención transfronteriza de pruebas se muestran WILLEMS, A.: "The Court of Justice of the European Union's Mutual Trust Journey in EU Criminal Law: From a Presumption to (Room for) Rebuttal", *German Law Journal*, 20, 2019, pp. 468 y ss., y AMBOS, K.: "Desarrollos y adaptaciones del principio de reconocimiento mutuo – Reflexiones sobre los orígenes de la orden europea de investigación con vistas a una comprensión práctica del principio de reconocimiento mutuo", en M. Llorente Sánchez-Arjona (Dir.). *Estudios procesales sobre el espacio europeo de justicia penal*, Cizur Menor: Aranzadi, 2021, pp. 141 y ss., esp. pp. 164 a 166.

cooperación transfronteriza[25], lo que desde luego conlleva sus riesgos, pues tales proveedores actuarán, obviamente, sobre todo en pro de su beneficio empresarial[26].

También se está pidiendo a los representantes de los proveedores de servicios que controlen la legalidad, necesidad y proporcionalidad de todas las órdenes que reciban, que podrán llegar a ser numerosísimas, así como el respeto de las garantías y derechos fundamentales de los afectados por ellas, tareas que, además de exceder de sus principales objetivos empresariales, deberán realizar en poco tiempo y disponiendo de muy pocos datos para decidir sobre esas cuestiones. Ya hemos indicado que las representaciones de los proveedores sólo recibirán Certificados, formularios sucintos, no las órdenes de entrega o conservación propiamente dichas redactadas por las autoridades de emisión competentes, en las que sí se explicitarían los motivos y fundamentos de la solicitud cursada.

La suma de todas estas circunstancias, unidas a las posibles sanciones pecuniarias y eventualmente penales a los proveedores que no cumplan con las órdenes de entrega y conservación, puede dar como resultado una ejecución masiva y *cuasi* automática de las órdenes de entrega y retención de información electrónica almacenada por los proveedores de

25. Más ampliamente MITSILEGAS: En el nuevo modelo se establece una relación entre las autoridades encargadas de la aplicación de la ley –*law enforcement*– y los actores privados –las compañías proveedoras de servicios–, los cuales, quieran o no, se convertirán en brazos ejecutores de las autoridades, reemplazando así a sus propias autoridades nacionales en la tarea de recibir, cumplir *y evaluar* las órdenes. Sin embargo, a diferencia de las autoridades nacionales, los proveedores de servicios deberán cumplir con esas funciones que se les enconmiendan *bajo la amenaza de sanciones por incumplimiento*, lo que hará que estos proveedores de servicios no puedan ser considerados fiables defensores de nuestros derechos fundamentales, concluye el autor. *Vid.* su trabajo "The privatisation of mutual trust in Europe's area of criminal Justice: The case of e-evidence", *Maastricht Journal of European and Comparative Law*, 2018, pp. 263 y ss., esp. p. 264. También DANIELE muestra su preocupación por esta tendencia a la "privatización de la tutela de los derechos fundamentales" que afirma se observa también en esta propuesta de Reglamento, pues se confía al proveedor de servicios, esto es, a empresas privadas, el control sobre la ejecución de las órdenes, con argumentos "esencialmente de tipo utilitarista". Destaca el autor que esta exclusión de los órganos estatales del Estado de ejecución no es exclusiva de la propuesta de Reglamento, pues una disposición semejante se encuentra en la CLOUD Act de 2018, su homólogo estadounidense. Se trata por tanto de una fuerte tendencia, a nivel global, que justamente por eso ha de ser valorada con la máxima cautela, concluye el autor en su trabajo"L'acquisizione delle prove digitali dai service provider: un preocupante cambio di paradigma nella cooperazione internazionale", *Riv. Bras. Dir. Proc.*, 2019, pp. 1277 y ss. esp. p. 1289.

26. Muy interesantes las reflexiones a este respecto de TOSZA en su trabajo "Internet service providers as law enforcers and adjudicators. A public role of private actors", *Computer Law & Security Review,* 43 (2021), pp. 1 y ss.

servicios, sin muchas más consideraciones, por lo que *de facto* se estaría prescindiendo del doble control de legalidad y de respeto de los derechos fundamentales, garantías que hasta ahora ha venido operando en la cooperación transfronteriza en la UE. Sería sin duda un cambio de paradigma, un verdadero giro copernicano en la materia; de "salto cuántico" lo ha calificado TOSZA[27].

En todo caso, sí le reconocemos una notable virtud a esta propuesta normativa: pretende superar el criterio de la territorialidad en materia de obtención transfronteriza de pruebas electrónicas. Según se expuso en los párrafos precedentes, no podemos seguir aplicando ese criterio cuando hablamos de la necesidad de obtener información electrónica, pues no está vinculada a un territorio concreto; está "en la nube", en servidores de distintos países, incluso almacenada de forma itinerante o fragmentada. Por lo tanto, en efecto, el referente en la cooperación ha de ser el proveedor de servicios; si éste opera en Estados de la Unión, tenga o no en ellos su sede o establecimiento, vendrá obligado a colaborar en la investigación y enjuiciamiento de hechos delictivos en la Unión, y tendrá que hacerlo designando al menos un representante a esos efectos.

Sin embargo, consideramos que lo antedicho no impide que siga existiendo un doble control por parte de las autoridades judiciales competentes, en el Estado de emisión y también en el Estado de ejecución. Tal control doble habrá de conjugarse de la forma más eficaz posible con el requisito de celeridad que exige la obtención de una prueba de estas características, muy volátil, muy frágil, muy fácil de trasladar.

Esta conjunción o equilibrio necesario entre eficacia, rapidez y garantías[28] se ha intentado alcanzar precisamente por parte de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento

27. Destaca el autor que en este tipo de órdenes para la obtención transfronteriza de *e-evidence* se está exigiendo un nivel de confianza en la autoridad de emisión mucho más alto que el existente hasta ahora, por lo que se produciría un "*quantum leap*", sin la suficiente armonización de garantías procesales, de los recursos disponibles para los afectados y de otros elementos que deberían sustentar esa confianza, como por ejemplo una mayor aproximación de la legislaciones en materia de "*privacy*". Eso por no mencionar el insatisfactorio nivel del "*rule of law*" en ciertos países, que de hecho actualmente afecta a la propia ejecución de los instrumentos de cooperación ya asentados sobre el reconocimiento mutuo, concluye el autor en "All evidence is equal…", *op. cit*., p. 181.

28. Como afirma DE BUSSER, cierto es que el sistema diseñado en este "*E-evidence package*" podría convertirse en una suerte de "*Fast-Track Line*" para pruebas electrónicas si se compara con el de la Directiva sobre Orden Europea de Investigación, pero deberíamos tener claro que no podemos optar por la rapidez a cualquier precio. *Vid.* "EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow", *German Law Journal*, Vol. 19, Issue 5, 2018, pp. 1251 y ss., esp. p. 1266.

europeo, quien en su relevante informe fechado el 11 de diciembre de 2020[29] formuló, entre otras propuestas de mejora, las que sintetizamos a continuación:

Las órdenes de entrega y conservación se deberán remitir *directa y simultáneamente* al proveedor de servicios y a la autoridad judicial que designe la legislación del Estado de ejecución. Así, tras la recepción del EPOC a fin de obtener datos de abonados y/o direcciones IP para identificar a una persona, *Vid.* art. 8 bis[30], el proveedor de servicios garantizará la transmisión de los datos a la autoridad de emisión en un plazo máximo de 10 días, o en 16 horas en caso de urgencia. La información simultánea de esta solicitud a la autoridad de ejecución "no tendrá efecto suspensivo en lo que respecta a las obligaciones del proveedor de servicios", pero si la autoridad de ejecución decidiera invocar, dentro de esos plazos, alguno de los motivos de no reconocimiento o no ejecución de los previstos en el Reglamento, informará inmediatamente a la autoridad de emisión y al proveedor de servicios. En el caso de que la autoridad de emisión ya hubiera recibido los datos, deberá suprimirlos y por tanto no podrá emplearlos; si aún no se hubieran transmitido, el proveedor de servicios se abstendrá de hacerlo. El art. 9 sería el relativo a la ejecución del EPOC cuando se solicitan datos de tráfico y/o de contenido, certificado que también se remitiría simultáneamente al proveedor de servicios y a la autoridad de ejecución. Como en el supuesto anterior, esta última podrá denegar la entrega de esos datos por alguna de las causas previstas en el propio Reglamento.

En el caso de EPOC-PR, que igualmente sería remitido directa y simultáneamente al proveedor de servicios y a la autoridad de ejecución, *Vid.* art. 10, la información a la autoridad de ejecución no tendría efecto suspensivo de las obligaciones del proveedor, de tal manera que, una vez recibido el certificado, éste debería actuar sin demora para conservar los datos solicitados. La conservación podrá mantenerse hasta un máximo de 60 días, más una prórroga de otros 30 si fuera necesaria una nueva evaluación de la pertinencia de los datos. Si el proveedor de servicios considera que el EPOC-PR está incompleto, contiene errores manifiestos, no contiene información suficiente para ejecutarlo, o es claramente abusivo, lo comunicará a la autoridad de emisión y de ejecución, a fin de que ésta solicite aclaraciones a la primera.

29. "Informe sobre la Propuesta de Reglamento del Parlamento europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal", Comisión LIBE, Ponente: Birgit Sippel, COM (2018) 0225 – C8-0155/2018 – 2018/0108(COD).

30. En los párrafos siguientes las referencias serán al articulado de la propuesta de Reglamento tal y como quedaría tras las modificaciones que indica el Parlamento en el Informe *supra* citado.

En conclusión, como se destaca en el propio Considerando 42.º ter 1, añadido por el citado Informe de la Comisión LIBE del Parlamento europeo: "Sin perjuicio del principio de confianza mutua, la autoridad de ejecución deberá tener la posibilidad de denegar el reconocimiento de la ejecución de una orden europea de entrega si dicha denegación se basa en el incumplimiento de las condiciones para la emisión de una orden europea de producción establecidas en el presente Reglamento o en los motivos específicos enumerados en el presente Reglamento".

A nuestro modo de ver, esta que se propone desde el Parlamento europeo puede ser una solución aceptable, pues mejoraría el modelo presentado por la Comisión en abril de 2018. Permitiría facilitar y agilizar la obtención transfronteriza de información electrónica, a la vez que se evitarían los ya apuntados problemas que seguro surgirían con la "privatización" del reconocimiento mutuo, pues se implantaría un control suficiente por parte de las autoridades competentes en ambos Estados, el de emisión y el de ejecución, en línea con los instrumentos hasta ahora empleados en materia de cooperación transfronteriza en la UE con base en el art. 82.1 TFUE y en el principio de reconocimiento mutuo.

Otra de las críticas que ha suscitado la propuesta de Reglamento presentada por la Comisión tiene que ver con que no se haga referencia en ella a la posibilidad de que también la defensa del investigado/acusado pueda solicitar la emisión de una de estas órdenes para la obtención de las pruebas electrónicas que ésta pudiera requerir; lo cual, por cierto, sí está previsto expresamente en la Directiva OEI, en su art. 1.3[31].

Como era de esperar, el primer colectivo profesional que alzó su voz en contra de esta carencia de la propuesta de Reglamento fue el de la Abogacía europea[32]. Concretamente el CCBE –*Council of Bars and Law Societies of Europe*[33]–, en el informe que hicieron público con fecha de 19 de octubre de 2018, y en relación con esta concreta cuestión[34], manifestaron que se

31. "La emisión de una OEI puede ser solicitada por una persona sospechosa o acusada (o por un abogado en su nombre), en el marco de los derechos de la defensa aplicables de conformidad con el procedimiento penal nacional".

32. También se manifestó en este sentido crítico la organización FAIR TRIALS, *Vid.* el citado informe *E-evidence Position Paper,* de 2019.

33. El CCBE –Consejo de la Abogacía Europea– representa a las Abogacías de 45 países y, a través de ellos, a más de 1 millón de abogados. El CCBE ya fue consultado por la Comisión antes de publicar su propuesta de Reglamento de abril de 2018, pero en este documento de octubre 2018 el CCBE amplió sus posiciones, a la vista de la concreta propuesta publicada por la Comisión.

34. *Posición del CCBE sobre la Propuesta de Reglamento de la Comisión sobre las Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos del enjuiciamiento penal, Vid*. esp. pp. 8 a 11. También puso de relieve el CCBE la importancia de preservar la

vulneraban los derechos de la defensa, la igualdad de armas y el juicio justo, ya que los Fiscales podían solicitar la emisión de una orden de entrega o conservación de datos de este tipo, pero no estaba previsto que los investigados/acusados, su defensa técnica, pudieran solicitar pruebas electrónicas a través de este instrumento de cooperación transfronteriza, lo que evidentemente "colocaba al acusado en una desventaja significativa"[35].

Por su parte, también la Comisión LIBE del Parlamento europeo en el Informe citado ha demandado expresamente que se incluya una previsión en aras de la vigencia de los referidos derechos de defensa e igualdad de armas. Así, propone que complete el articulado del Reglamento en este sentido: Art. 1 bis: "La emisión de una orden europea de entrega o de conservación podrá asimismo ser solicitada en nombre de una persona sospechosa o acusada, en el marco de los derechos de la defensa aplicables de conformidad con los procedimientos penales nacionales".

Suscribimos plenamente estas propuestas coincidentes de la Abogacía europea, de la organización no gubernamental *Fair Trials* y de la Comisión LIBE del Parlamento europeo. No obstante, desde la concreta perspectiva del proceso penal español, en el que también las víctimas pueden ejercitar la acción penal[36], sería deseable que se incorporara al texto que finalmente

---

confidencialidad de las comunicaciones abogado-cliente cuando se solicita conocer el contenido de una comunicación electrónica y, en consecuencia, "Si los datos están cubiertos por obligaciones de secreto profesional, la EPO no debe emitirse", pp. 19 y 20. Para facilitar que los proveedores de servicios conozcan en qué casos concurre esta circunstancia, el CCBE propone ayudar a crear un mecanismo que identifique abogados, previa recopilación de los listados de profesionales que suministren los propios Colegios profesionales. Este tipo de herramientas ya se utilizan en el contexto del sistema *e-Codex*, que entre otras utilidades ofrece una infraestructura digital para una comunicación transfronteriza segura en materia de justicia; *Vid*. más ampliamente la información contenida en: https://www.e-codex.eu.

35. Igualmente. muy rotundo en este sentido crítico, el Informe de FAIR TRIALS de 2018, p. 5: "The proposal, as drafted, is entirely one-sided. On the one hand, prosecutors can issue preservation orders at will and production orders for most offences. And on the other, no provisions exist to enable defendants to use or deal with electronic evidence. The proposal undermines the principle of equality of arms between prosecution and defence, placing the defendant at a significant disadvantage. Moreover, the draft legislation does not guide service providers in limiting disclosure of data to information that is relevant for the purposes of the criminal investigation. As drafted, the Orders could result in LEAs being swamped with data –and there is no provision to ensure that defendants don't in turn get snowed under the weight of the e-evidence in their case file– making it difficult, if not impossible, to prepare and exercise effectively their defence. This is particularly worrisome for indigent defendants in the light of the trend across the EU to cut back on legal aid".

36. Sobre esta cuestión, *in extenso*, DE HOYOS SANCHO, M.: *El ejercicio de la acción penal por las víctimas. Un estudio comparado*, Cizur Menor: Aranzadi, 2016.

se apruebe la posibilidad de que las acusaciones personadas en la causa soliciten la emisión de una orden europea de entrega o conservación de la información electrónica que eventualmente pudieran necesitar en defensa de sus propias pretensiones procesales.

Por lo que respecta a los motivos de denegación del reconocimiento o ejecución de una orden de entrega contenida en el correspondiente EPOC, la Comisión LIBE del Parlamento europeo ha propuesto que se añada[37], en el que sería el nuevo art. 10 bis, una referencia expresa y como motivo de denegación *obligatorio* –no facultativo, como en la propuesta de la Comisión– a la obligación de respetar los derechos fundamentales y principios jurídicos de la Carta y del art. 6 del TUE, incluido el derecho de defensa.

También debería ser un motivo de denegación *obligatorio* que la ejecución de la orden de entrega resultara contraria al principio "*ne bis in idem*", tal y como se reconoce en la Carta y desarrolla la jurisprudencia del TJUE. Así lo recoge el Considerando 42 ter del propio Informe del Parlamento europeo.

Igualmente se propone la incorporación de una referencia a la vulneración de la inmunidad o privilegio procesal en el Estado de ejecución como motivo de denegación *obligatorio* por la autoridad de ejecución[38], con especial alusión a las normas sobre limitación de la responsabilidad penal en relación con la libertad de prensa y de expresión conforme a la legislación del Estado de ejecución[39].

Además, entre otros motivos facultativos de denegación de la ejecución, concretamente en relación con un EPOC solicitando la entrega de datos de tráfico y de contenido, la referida Comisión LIBE propuso los siguientes –art. 10 bis, apdo. 2.º–: b) "Cuando la orden europea de entrega se refiera a una infracción penal presuntamente cometida fuera del Estado emisor, y total o parcialmente en el de ejecución, pero la conducta que dio origen a la emisión del EPOC no era constitutiva de infracción penal con arreglo a la legislación del Estado de ejecución. c) Cuando la conducta que dio origen a la emisión del EPOC no fuera constitutiva de infracción con arreglo a la legislación del Estado de ejecución, y no se trate de una de las

37. *Vid*. Considerando 42 *quáter*.

38. Tengamos en cuenta en este punto la importancia de que se preserve el "privilegio" que conlleva el derecho a la necesaria confidencialidad de las comunicaciones entre abogado y cliente. Sobre el particular, ampliamente, BACHMAIER WINTER, L. y MARTÍNEZ SANTOS, A. (Dirs.): *Asistencia letrada, confidencialidad abogado-cliente y proceso penal en la sociedad digital. Estudio de Derecho comparado*. Madrid: Marcial Pons, 2021.

39. Véase el Considerando 42 *quinquies*.

categorías delictivas del Anexo III bis[40], conforme indique la autoridad emisora del EPOC, siempre que en el Estado de emisión fuera punible con pena privativa de libertad o internamiento de una duración máxima no inferior a los 3 años. d) Cuando la ejecución de la orden europea de entrega esté limitada, con arreglo a la legislación del Estado de ejecución, a una lista o categoría de infracciones, o infracciones con un umbral más limitado".

Tras la lectura de lo previsto en los anteriormente transcritos apartados b), c) y d), puede concluirse que se propone una incorporación al texto del Reglamento del principio o exigencia de "doble incriminación", que según indicamos *supra* ha venido siendo reclamado también en materia de cooperación transfronteriza para la obtención de pruebas electrónicas[41], y que no había encontrado reflejo en la propuesta de Reglamento inicialmente presentada por la Comisión europea en abril de 2018.

Estamos totalmente de acuerdo con tal inclusión, pues no sería de recibo que, más allá de los clásicos 32 tipos delictivos que se presumen castigados en todos los Estados de la Unión y cuando la pena de privación de libertad prevista fuera superior a los tres años, se permitiera la entrega de información electrónica a una autoridad extranjera sin ese control de "doble incriminación"; es decir, que se obligara al proveedor de servicios a entregar información en supuestos en los que no se le podría haber solicitado ésta por una autoridad del propio Estado de ejecución, por no ser allí punible esa conducta.

En cuanto a los medios de impugnación que pudieran emplear las personas cuyos datos se han buscado mediante orden europea de entrega o conservación, la referida Comisión LIBE propone, de acuerdo con el sistema de doble control que pretende quede establecido –*Vid.* Considerando 54 de su Informe– que se puedan emplear las "vías de recurso efectivas"

40. Que contiene la clásica referencia a las treinta y dos "categorías de infracciones" exentas del control de doble incriminación, precisamente porque se presupone que todos esos tipos delictivos graves son punibles en todos los Estados de la Unión –criminalidad organizada, terrorismo, trata de seres humanos, homicidio, delitos informáticos, etc.–. Ya en su día el Supervisor Europeo de Protección de Datos, en su Informe de 2020, manifestó que "estaría a favor de definir una lista exhaustiva de infracciones graves que justificaran la emisión de órdenes europeas de entrega para obtener datos de transacciones y datos de contenido, ya que esto aumentaría también la seguridad jurídica de todas las partes interesadas participantes". *Vid. Dictamen sobre las propuestas relativas a las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal*, DOUE 31.1.2020, C 32/11.

41. Véase en particular el citado Informe del CCBE de 2018, p. 7, así como las conclusiones de TINOCO PASTRANA, "Las órdenes europeas de entrega y conservación…", *op. cit*., p. 245.

en relación con la legalidad, necesidad y proporcionalidad de las órdenes, tanto en el Estado emisor como en el de ejecución, de conformidad con las respectivas legislaciones nacionales, *Vid*. art. 17, apdo. 3. No obstante, los motivos de fondo por los que se emitió la orden únicamente podrán ser impugnados en el Estado de emisión, que es donde se tramita la causa penal; "sin perjuicio de las garantías de los derechos fundamentales en el Estado de emisión", se indica como tenor del que sería el apdo. 3 bis de este art. 17.

III. EL SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO DE BUDAPEST CONTRA LA CIBERCRIMINALIDAD, EN EL MARCO DEL CONSEJO DE EUROPA

El 2.º Protocolo adicional al Convenio sobre ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas[42] –STCE núm. 224– fue adoptado por el Comité de Ministros del Consejo de Europa el 17 de noviembre de 2021, y ha sido suscrito hasta la fecha en que se redactan estas líneas por un total de 24 Estados[43], entre los que se encuentran, además de países miembros del Consejo de Europa y de la Unión Europea[44], otros que no lo son, pero que tienen incuestionable

42. Pueden leerse algunas valoraciones sobre el instrumento en: VELASCO NÚÑEZ, E.: "El Segundo Protocolo Adicional del Convenio de Budapest contra la cibercriminalidad", y DELGADO MARTÍN, J.: "Presente y futuro de la prueba digital internacional. El Segundo Protocolo Adicional del Convenio de Budapest contra la cibercriminalidad", ambos trabajos publicados en el *Diario La Ley*, de 24 de mayo de 2022. En ese mismo ejemplar del *Diario La Ley* se publicó una entrevista a D.ª Elvira Tejada, Fiscal de Sala Coordinadora contra la criminalidad informática, comentando el instrumento en cuestión. *Vid.* también el artículo de la Fiscal BAHAMONDE BLANCO, quien representó a nuestro M.º de Justicia en las negociaciones del instrumento: "Segundo Protocolo Adicional al Convenio de Budapest: Nuevos medios para la cooperación penal y la obtención de prueba electrónica", *La Ley Penal*, núm. 157, julio-agosto 2022. Más recientemente se ha ocupado de específicamente del tema GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E.: "El nuevo Protocolo del Convenio de Budapest de lucha contra la criminalidad", *Revista General de Derecho Procesal*, núm. 58, 2022, pp. 1 y ss.

43. España lo firmó el 15 de mayo de 2022. La entrada en vigor se producirá cuando se alcancen al menos cinco ratificaciones.

44. Por medio de la Decisión (UE) 2022/722 del Consejo, de 5 de abril de 2022, se autorizó a los Estados miembros de la Unión Europea a firmar, en interés de la Unión, este 2.º Protocolo adicional. Téngase en cuenta además lo dispuesto en el art. 15 apdo.1.b) del mismo instrumento: "Las Partes que también sean miembros de la Unión Europea podrán, en sus relaciones mutuas, aplicar el Derecho de la Unión Europea que regule las cuestiones tratadas en el presente Protocolo", de tal manera que si en el futuro entra en vigor el Reglamento UE sobre conservación y entrega de pruebas electrónicas, con un sistema de cooperación más sencillo y más rápido, con fundamento en el

relevancia en la materia que nos ocupa, como los Estados Unidos o algunos países del ámbito iberoamericano.

La aprobación de este instrumento se justifica, según puede leerse en el Preámbulo, en la proliferación de la cibercriminalidad[45] y en la creciente complejidad de la obtención de pruebas electrónicas, que pueden estar almacenadas en jurisdicciones extranjeras, múltiples, cambiantes o desconocidas, al tiempo que los poderes de los servicios estatales de persecución de los delitos se encuentran limitados en sus funciones por las fronteras territoriales.

Precisamente para salvar estas dificultades en lo posible, el referido 2.º Protocolo adicional establece una base jurídica internacional que vendrá a reforzar la *cooperación entre las autoridades de una Parte y los proveedores de servicios que se encuentren en el territorio de otra Parte,* quienes podrán ser requeridos de manera directa[46] para la entrega de información sobre el registro de nombres de dominio o datos de abonados que tengan almacenados, o bien a través de la autoridad competente del Estado requerido si lo que se solicitan son datos relativos al tráfico. También recoge una modalidad de cooperación inmediata todavía más amplia para supuestos de emergencia, al tiempo que se establecen garantías para los derechos fundamentales, en particular en materia de protección de datos personales.

La posibilidad de obtener directamente de los proveedores de servicios información sobre los datos de abonados ya se encontraba en el art. 18 del propio Convenio de Budapest de 2001[47], pero se excluía expresamente la posibilidad de que estos proveedores ofrecieran datos sobre el tráfico o sobre el contenido[48].

---

reconocimiento mutuo, los Estados UE preferirán que en sus relaciones de cooperación transfronteriza en la materia se aplique tal Reglamento.

45. Si bien se indica expresamente que este Protocolo es de aplicación también para la obtención "de pruebas electrónicas *de cualquier delito*", *Vid.* art. 2, apdo. 1.º.

46. Indica GUDÍN RODRÍGUEZ-MAGARIÑOS que, aunque no se mencione expresamente, el "principio de ubicuidad" es la clave de este Convenio, de tal manera que cualquier Estado en el que se manifieste la cibercriminalidad, debe dotar a sus autoridades de las facultades necesarias para el acceso a los datos que custodian las empresas, dentro o fuera de sus respectivos territorios. *Vid.* su trabajo *supra cit.,* pp. 18 y ss.

47. Ratificado por España el 14 de septiembre de 2010, B.O.E del 17 de septiembre. *Vid.* las valoraciones sobre lo que ha supuesto la vigencia del instrumento en estos años, y en particular la creación de la Red 24/7, en BUJOSA VADELL, L.: "Cooperación judicial para la obtención…", *op. cit.,* pp. 74 y ss.

48. Artículo 18. Orden de presentación:

"1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a) A una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en

Las principales novedades que aporta este 2.º Protocolo Adicional, que sigue basándose en el tradicional principio "*favor cooperationis*"[49] y en la exigencia de la doble incriminación[50], en lo que respecta a la obtención transfronteriza de pruebas electrónicas, son las siguientes[51]:

El art. 6 es el relativo a la "*Solicitud de información sobre el registro de nombres de dominio*", y dispone que cada Estado Parte deberá adoptar las medidas legislativas y de otro tipo que fueran necesarias para que sus autoridades puedan cursar una petición de este tipo a entidades que presten servicios de registro de nombres de dominio en el territorio de otra Parte, a fin de hallar al registrante de un nombre de dominio o para poder ponerse en contacto con él, "a efectos de investigaciones o procesos penales específicos". Cada parte deberá adoptar las medidas necesarias para permitir que tales entidades revelen esa información cuando reciban una solicitud de estas características.

En el art. 7 se aborda la cuestión de la "*Revelación de información relativa a abonados*", precepto que también exige a las Partes que adopten las medidas necesarias para que se pueda emitir un requerimiento directamente a

---

un sistema informático o en un medio de almacenamiento de datos informáticos; y b) a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.

2. Los poderes y procedimientos mencionados en el presente artículo están sujetos a lo dispuesto en los artículos 14 y 15.

3. A los efectos del presente artículo, por «datos relativos a los abonados» se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, *excluidos los datos sobre el tráfico o sobre el contenido*, y que permita determinar:

a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios; c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios".

49. Así, en el art. 5 de este 2.º Protocolo se insta a las Partes a seguir colaborando "en la mayor medida posible".

50. Bien entendido que este requisito se cumple, según puede leerse en el art. 5, apdo. 6.º, con independencia de que la legislación de la Parte requerida incluya el delito en la misma categoría delictiva o lo denomine con la misma terminología que la Parte requirente, "si el acto subsumible en el tipo delictivo respecto del que se solicita la asistencia constituye delito con arreglo a su legislación".

51. Este instrumento también se ocupa de otras cuestiones relevantes en materia de asistencia transfronteriza en investigaciones o causas penales, como son los requisitos de uso de la videoconferencia –art. 11–, de los equipos conjuntos de investigación, de las investigaciones conjuntas –art. 12–, o de la protección de datos de carácter personal –art. 14–.

un proveedor de servicios que se encuentre en el territorio de otra Parte, a fin de que suministre información específica por ellos almacenada o bajo su control relativa a abonados, igualmente "para investigaciones o procesos penales específicos de la Parte emisora". Añade este precepto en el apdo.1.b) que en la firma o ratificación del instrumento las Partes pueden exigir que estos requerimientos a los proveedores de servicios que se encuentren en su territorio sean dictados "por un fiscal u otra autoridad judicial, o estar bajo su supervisión, o ser dictado bajo supervisión independiente".

El art. 8 se dedica a la posibilidad de "Dar efecto a los requerimientos de la otra Parte para la *presentación rápida de información relativa a abonados y datos relativos al tráfico*", específicos y almacenados, que obren en poder o estén bajo el control de dicho proveedor de servicios y sean necesarios para investigaciones o procesos penales específicos de ese Estado. La Parte requerida de colaboración "aplicará una diligencia razonable para dar traslado al proveedor de servicios en un plazo de cuarenta y cinco días, o antes si fuera posible" y ordenará a tal proveedor que se le entregue la información o datos solicitados –*Vid.* art. 8, apdo. 6.º–, en veinte días si es información sobre abonados, y en cuarenta y cinco si son datos relativos al tráfico[52].

También está prevista la "*Revelación rápida de datos informáticos almacenados en caso de emergencia*[53]" –art. 9–, haciendo uso de los respectivos "puntos de contacto de la Red 24/7[54]" a los que se refería ya el art. 35 del Convenio, de tal manera que a través del respectivo punto de contacto nacional se transmita la solicitud de información electrónica al homólogo de la otra Parte, con el fin de que éste requiera a un proveedor de servicios que se encuentra en el territorio de dicha Parte para que revele "de forma

52. Se prevé también la posibilidad de que la Parte requerida se niegue a ejecutar la solicitud si concurren motivos del art. 25, apdo. 4.º, o en el art. 27, apdo. 4.º del Convenio de Budapest: se consideran delitos "políticos", o la ejecución de la solicitud atenta contra la soberanía, seguridad, orden público u otros intereses esenciales de la Parte. Importante es destacar también lo dispuesto en el art. 25.5 del Convenio y en semejantes términos en el art. 5, apdo. 6.º del 2.º Protocolo Adicional: "Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia constituya un delito en virtud de su derecho interno, con independencia de que dicho derecho incluya o no el delito dentro de la misma categoría de delitos o lo denomine o no con la misma terminología que la Parte requirente". Bastará entonces con que los elementos objetivos y subjetivos del tipo respecto del que se solicita la asistencia constituyan delito con arreglo a su legislación.

53. Por situación de emergencia se entiende, según el art. 3.c): riesgo significativo e inminente para la vida o la seguridad de una o más personas físicas.

54. En España tal "Red 24/7" está radicada en la Comisaría General de Policía Judicial del Ministerio del Interior.

rápida *datos informáticos específicos* almacenados que obren en su poder o estén bajo su control, sin necesidad de presentar una solicitud de asistencia mutua". Por lo tanto, como este art. 9 del instrumento no distingue entre tipos de datos informáticos, ha de entenderse que en tales casos de emergencia podrán obtenerse a través de la Red 24/7, datos de abonados, de tráfico, e incluso de contenido, siempre que ya estén almacenados[55].

Es probable que este cauce de la asistencia mutua en situaciones de emergencia, definidas con cierta amplitud en el art. 3.c) del instrumento –riesgo significativo e inminente para la vida o la seguridad de una o más personas físicas–, sea muy utilizado en la práctica de la cooperación internacional. Además del citado art. 9, el art. 10 añade un considerable margen de actuación en tales situaciones de emergencia para demandar asistencia a través de la Red 24/7, por la versatilidad de las diligencias investigadoras que admite sean solicitadas en esos casos, que podrán ser de cualquier tipo, y porque la transmisión de la solicitud se simplifica mucho a través de los propios miembros de la Red[56].

Finalmente, sobre la eficacia esperable de este 2.º Protocolo adicional, debemos recordar que para su entrada en vigor se tiene que ratificar por los Estados Parte, al menos por cinco, cosa que no ha sucedido hasta la fecha y, además, los firmantes tendrán que introducir en sus respectivas legislaciones nacionales los cambios que fueran necesarios para dotar de efectividad al instrumento internacional. Es decir, los Estados Parte deberán facultar de manera expresa a los proveedores de servicios que se encuentren en su territorio para revelar directamente la información requerida por la autoridad competente extranjera.

De otro lado, como han destacado ya algunos analistas[57], el instrumento prevé un amplio catálogo de posibles declaraciones y reservas, a

55. Esta es la interpretación que hace BAHAMONDE BLANCO del art. 9 del 2.º Protocolo adicional, en cuyas negociaciones participó como Fiscal en representación del Ministerio de Justicia español. *Vid.* su trabajo "Segundo Protocolo adicional…", *op. cit*., p. 12. También en ese sentido VELASCO NÚÑEZ, E.: "El Segundo Protocolo adicional…", *op. cit.* p. 4: en caso de emergencia el proveedor tecnológico extranjero requerido deberá ceder rápidamente los datos electrónicos específicos almacenados en su poder; "no indica la norma cuáles, luego no se excluye ninguno". En consecuencia, a través del contacto de la Red 24/7 podrán pedirse "incluso datos de contenido", concluye el referido Magistrado de la Audiencia Nacional.

56. Es posible el contacto directo e inmediato entre ellos y además la documentación necesaria se restringe a la mínima expresión; se puede hacer uso de medios electrónicos de transmisión, e incluso cursar la solicitud verbalmente, con confirmación electrónica ulterior. *Vid.* GUDÍN RODRÍGUEZ-MAGARIÑOS, "El nuevo Protocolo del Convenio…", *op. cit.,* p.32.

57. *Vid.* BAHAMONDE BLANCO, M., *op. supra cit*., pp. 5 y 19, así como GUDÍN RODRÍGUEZ-MAGARIÑOS, *op. supra cit.,* pp. 44 y ss.

fin de que pueda adaptarse a los distintos sistemas jurídicos en que se aplicará, lo que le dotará de la necesaria flexibilidad. Sin embargo y al mismo tiempo, tal característica implica que hasta el momento en que se produzcan las respectivas ratificaciones, hasta que no conozcamos los concretos términos de las mismas, no podremos valorar toda la operatividad de estas nuevas herramientas de cooperación internacional. Las reservas y declaraciones determinarán cuestiones de tanta trascendencia como quiénes serán las concretas autoridades competentes para ejercer algunas de las funciones previstas en el texto, las opciones que ofrece cada uno de los preceptos[58], o la amplitud y alcance de las respectivas garantías.

En cualquier caso, este 2.º Protocolo adicional al Convenio de Budapest conlleva a nuestro juicio un claro avance, pues se amplía y actualiza el referido Convenio, que ha resultado ser muy eficaz en la práctica, al tiempo que se recogen en un instrumento normativo internacional y se garantizan algunas prácticas de cooperación transfronteriza en materia penal que ya se estaban llevando a cabo, en ocasiones basadas en Acuerdos bilaterales[59], como las colaboraciones directas y voluntarias prestadas por algunos proveedores de servicios radicados fuera del territorio del Estado reclamante en relación con peticiones de datos de abonados o incluso de tráfico[60].

58. Como ejemplo podemos mencionar el hecho de que los datos de abonados se podrán solicitar directamente al proveedor de servicios invocando el art. 7, pero también puede resultar que sea obligatorio cursar tal petición a través de las autoridades competentes de la Parte requerida, en los supuestos en que ese Estado Parte hubiera decidido que para obtener tal información será de aplicación el art. 8, y no el art. 7. *Vid.* los comentarios de D.ª Elvira Tejada en la publicación de la entrevista *supra* citada, p. 8.
59. Como en el importante Acuerdo de asistencia judicial entre los Estados Unidos de América y la Unión Europea, firmado el 25 de junio de 2003.
60. Colaboraciones que vienen prestando esos importantes proveedores de servicios de internet, o no, con base en sus propios criterios y respectivas políticas empresariales y de privacidad. *Vid.* la *Guía Práctica sobre preservación y obtención en Estados Unidos de datos de Internet,* p. 69, en su versión de 2019, parcialmente actualizada en 2021 y elaborada por la Magistratura de Enlace de España en Estados Unidos.