IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

La Directiva Europea y las Órdenes de Producción y Conservación de pruebas electrónicas en los procesos penales. ¿Nuevas perspectivas?*

THE EUROPEAN DIRECTIVE AND THE PRODUCTION AND PRESERVATION ORDERS OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS. NEW INSIGHTS?

Carmen Cuadrado Salinas
Profesora Contratada Doctora (Profesora Titular Acreditada) de Derecho Procesal.
Universidad de Alicante
carmen.cuadrado@ua.es 0000-0001-7824-4791

Recibido: 01 de noviembre de 2023 | Aceptado: 06 de diciembre de 2023

RESUMEN

Las medidas procesales para obtener y conservar pruebas electrónicas son cada vez más importantes a los efectos de las investigaciones y procesos penales a lo largo de la Unión Europea. Si tenemos en cuenta que los datos electrónicos se almacenan a menudo fuera del Estado investigador, o por un prestador de servicios establecido fuera de dicho Estado, es fácil comprender los enormes problemas que puede generar su obtención. El presente estudio analiza los recientemente aprobados instrumentos legales europeos, diseñados para resolver estos problemas: la Directiva y el Reglamento que contiene las Órdenes europeas de Producción y Conservación de pruebas electrónicas.

PALABRAS CLAVE

Obtención de pruebas tecnológicas
proveedores de servicios
Directiva
Orden Europea de Obtención de Pruebas Electrónicas
Orden Europea de Conservación de Pruebas Electrónicas

ABSTRACT

Procedural measures to obtain and preserve electronic evidence are increasingly important for the purposes of criminal investigation and prosecution across the European Union. If we tale into account that electronic data is often stored outside the investigating State, it is easy to understand the huge problem that gathering of these data, as evidence can generate. This study analyzes the recently approved legal instruments, designed to solve these problems: the Directive and the Regulation on European Production Orders and European Preservation Orders.

KEYWORDS

Gathering of electronic evidence
service providers
Directive
European Production Orders for Electronic Evidence
European Preservation Orders for Electronic Evidence

* Trabajo realizado en el marco de los Proyectos de Investigación "Empresa y proceso. Investigación y Cooperación" (Ref. PID 2020-119878GB-100) del Ministerio de Ciencia e innovación.

I. Consideraciones previas

El 28 de julio de 2023, el Diario Oficial de la Unión Europea (DOUE) ponía fin al largo camino iniciado en 2016, al publicar la nueva y esperada normativa relativa a la obtención de pruebas transfronteriza dentro de un proceso penal, a través de dos instrumentos conexos muy específicos: por un lado, el Reglamento 2023/1543, de 12 de julio (en adelante el Reglamento), sobre las órdenes europeas de producción y de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de los procesos penales; y, por otro, la Directiva 2023/1544, de 12 de julio (en adelante la Directiva), por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales, ambos del Parlamento Europeo y del Consejo, cuyo plazo de transposición en los ordenamientos de los Estados miembros es el 18 de febrero de 2026, como máximo.

La exigencia de una nueva normativa, a pesar de estar en vigor la Orden de Investigación Europea (OIE)[1], viene originada por varios factores entre los que se encuentra, principalmente, la poca o nula eficacia de este último instrumento a la hora de recabar las pruebas electrónicas, en un ámbito en el que ya está generalizado el uso de dispositivos electrónicos como medio para la comisión de cualquier delito. La naturaleza volatil de los datos electrónicos, por otro lado, no casa bien con las dilaciones derivadas de los plazos y la burocracia provocada por los procedimientos de cooperación judicial en los que se basa la mencionada OIE, y en definitiva, el problema al que nos enfrentábamos era la ausencia de una normativa específica que permitiese la obtención de pruebas electrónicas de ámbito transfronterizo, –puesto que los datos que los investigadores pueden necesitar se encuentra almacenada en servidores distribuidos en distintos Estados– hacía muy difícil, sino imposible, alcanzar estos objetivos con la única ayuda de la OIE (De HOYOS, 2023, p. 101).

Uno de los mayores escollos, pues, en el ámbito de la obtención de pruebas digitales, se encontraba en la ausencia de un régimen común de protección de datos en el ámbito penal entre los Estados miembros, frente al amplio abanico normativo existente, y por ello muy disperso, de estándares legales en las diferentes legislaciones procesales en relación a la obtención de pruebas, y, además, sin la implementación de unas reglas comunes relativas a las garantías procesales mínimas y básicas que el sujeto investigado debía tener en todos y cada uno de los Estados miembros[2]. (PEERS, S., 2010 y SAYERS, D., 2011).

1. Directiva 2014/41/UE del Parlamento y del Consejo, de 3 de abril, relativa a la Orden Europea de Investigación en Materia Penal (DOUI de 1 de mayo de 2014, que se creó con la finalidad de reemplazar dos instrumentos jurídicos hasta entonces vigentes, y con la intención de evitar duplicidades en materia de obtención de pruebas: la Decisión Marco del Consejo de Europa 2003/577/JHA, de 22 de julio, y la Decisión Marco 2008/978/JHA, de 18 de diciembre. La OIE tuvo como base el Programa de Estocolmo, adoptado por la Comisión Europea el 11 de diciembre de 2009. Si bien se recogía el acceso a pruebas electrónicas, la Orden no contenía disposición específica alguna sobre la obtención transfronteriza de pruebas electrónicas.

2. Entre otros pueden verse los informes presentados ante la Comisión Europea de *Fair Trials International* "Fair Trials International's response to a European Member States's legislative initiative for

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

La práctica de los operadores jurídicos durante las labores de búsqueda de elementos probatorios en el proceso penal puso en evidencia que el 85% de las investigaciones penales conlleva el uso de dispositivos electrónicos, y de estos, más de la mitad contienen una petición transfronteriza de acceso a pruebas electrónicas. Por ello, en sus Conclusiones sobre la mejora de la justicia penal en el ciberespacio, el Consejo advirtió de la necesidad de desarrollar acciones concretas basadas en un enfoque común de la UE que facilitasen una asistencia jurídica mutua más eficaz; y lo que resultaba más novedoso pero también más desafiante, basado en el objetivo de establecer vías de cooperación más eficaces entre las autoridades de los Estados miembros y los proveedores de servicios radicados en países no pertenecientes a la UE, así como proponer soluciones al problema de la determinación y aplicación de la jurisdicción en el ciberespacio[3]. En este sentido, como bien señala ROGALSKI, "la propuesta de la Comisión intentaba alcanzar el extremadamente delicado equilibrio entre una eficaz y eficiente investigación penal (para la policía judicial y el juez de instrucción), certeza jurídica (para las compañías tecnológicas), y la protección de los derechos fundamentales (para el sospechoso y otros usuarios)" (ROGALSKI, 2020, p. 335).

Por su parte, el Parlamento Europeo también manifestó expresamente que la creación de un marco jurídico de armonización dirigido a la creación de deberes de colaboración a los proveedores de servicios, con la obligación de dar cumplimiento a las solicitudes cursadas por los jueces, fiscales o fuerzas y cuerpos de seguridad, era todo un reto que había que lograr, abogando por la creación de un marco jurídico europeo armonizado que incluyese salvaguardias para los derechos y las libertades de los interesados[4].

La Comisión propondría, entonces, el 17 de abril de 2018, y mediante una Resolución, la elaboración de dos documentos conexos, uno con forma de propuesta de Reglamento (COM/2018/225) y otro con forma de propuesta de Directiva (COM/2018/226), con la declarada intención de crear la denominada Orden Europea de Entrega (EPOC) y una Orden de Preservación de Pruebas Electrónicas (EPOC-PR), ambas con fuerza vinculante, basadas en la posibilidad de que la autoridad judicial de un Estado Miembro solicite directamente a un proveedor de servicios –que se encuentre ubicado en otra jurisdicción–, los datos electrónicos necesarios para obtener pruebas en los procesos penales iniciados. La EPOC-PR, por su parte, solo permitirá solicitar la conservación de datos que ya se encuentren almacenados en el momento de la recepción de la orden y no podrá ser utilizada, en ningún caso, para acceder a datos producidos antes o tras la recepción de la orden. Ambos instrumentos fueron concebidos, pues, ante la necesidad de obtener pruebas electrónicas de carácter transfronterizo por no existir otros instrumentos eficaces frente al creciente e imparable desarrollo tecnológico y el problema relativo a la aplicación de los conceptos tradicionales en relación con la territorialidad y la jurisdicción (TOSZA, 2020, p. 168).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

---

a Directive on a European Investigation Order", de 29 de junio de 2010 disponible en http://www.statewatch.org/news/2010/jul/eu-eio-ft-briefing.pdf.

3. Conclusiones del Consejo de la Unión Europea, de 9 de junio de 2016, sobre la mejora de la justicia penal en el ciberespacio, ST9579/16.

4. P8_TA(2017)0366.

Con estas propuestas, la Comisión Europea puso en marcha una serie de negociaciones internacionales, en 2018, sobre el acceso a la prueba electrónica transfronteriza, dando así un paso tan decisivo como necesario para perseguir penalmente a organizaciones criminales y terroristas. En octubre de ese mismo año, la Comisión presentó dos propuestas de negociación de directivas: una para negociar con los EEUU[5], con base en un acuerdo bilateral aprobado por el Congreso de los EEUU en relación con la *Clarifying Lawful use of Overseas Data Act*, más conocida como CLOUD Act, de 23 de marzo de 2018. Este acuerdo formaba parte del denominado *Omnibus Spending Bill*, creando, de este modo, una base legal para que el gobierno de los EEUU pueda llegar a acuerdos con otros Estados en relación al acceso de datos contenidos y almacenados por proveedores de servicios norteamericanos y viceversa (FRANSSEN, 2018); y una segunda propuesta para negociar un segundo Protocolo Adicional del Convenio sobre Cibercrimen[6] y relativo a la cooperación reforzada y la revelación de pruebas electrónicas[7].

Este segundo Protocolo reconocía la necesidad de incrementar la cooperación de forma más eficiente, entre los Estados y los proveedores de servicio, en el contexto de obtención de pruebas de los delitos electrónicos, recogiendo ya la exigencia de dotar de una mayor seguridad jurídica a las investigaciones penales en relación con las circunstancias en las que puedan atenderse las solicitudes de las autoridades penales de otros Estados Parte en la revelación de datos electrónicos; así como garantizar una protección más efectiva contra la ciberdelincuencia y en la obtención de pruebas en formato electrónico garantizando, como no podía ser de otro modo, el respeto de los derechos y libertades fundamentales (De HOYOS, 2023, p. 118).

II. La designación de establecimientos y representantes legales a efectos de recabar pruebas para los procesos penales en la Directiva

Los atentados acaecidos en Bruselas el 22 de marzo de 2016[8] provocaron una urgente reunión conjunta de los ministros de Justicia y de Interior de los Estados miembros y de

5. Recomendación para la autorización de negociaciones con vistas a un acuerdo entre la Unión y los EEUU de América sobre acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en asuntos penales, de 5 de febrero de 2019 COM (2019) 70 final. Vide https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf

6. Recomendación para una decisión del Consejo sobre la autorización a participar en las negociaciones de un segundo Protocolo Adicional del Convenio Europeo sobre Cibercrimen (CETS No 185). De 5 de febrero de 2019 COM (2019) 71 final. Vide https://ec.europa.eu/info/sites/info/files/recommendation_budapest_convention.pdf

7. Adoptado por el Comité de Ministros del Consejo de Europa el 17 de noviembre de 2021. Abierto a la firma en Budapest el 23 de noviembre de 2001, España lo firmó el 12 de mayo de 2022. Publicado en el DOUE núm. 63, de 28 de febrero de 2023.

8. Atentado islamita que costó la vida a más de treinta personas y dejó heridos a más de 230. Se trató de un doble atentado que afectó al aeropuerto y el metro, y este último el artefacto explosivo estalló en la estación de Molenbeck, muy cerca del lugar donde está situada la Comisión y el Parlamento Europeo.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

los representantes de instituciones de la UE. Esta reunión sirvió para alcanzar el acuerdo de trabajar sin más dilación en la creación y desarrollo de las vías de actuación necesarias para permitir una cooperación más intensa y eficaz con los proveedores de servicios que operan no solo en el territorio europeo, sino también con terceros países.

La finalidad de fomentar y facilitar una mayor y más eficiente cooperación con los proveedores de servicios se dirigía a posibilitar, no solo la obtención, sino también el aseguramiento, a través de una orden de conservación, de quienes tuviesen la posesión de cualquier dato electrónico que las autoridades investigadoras necesitasen. Y estos acuerdos se volcaron como conclusiones en el Documento que publicó el Consejo de 9 de junio de 2016[9]. Tras ello se solicitó a la Comisión la elaboración de un estudio que sirviese de base a una propuesta con la finalidad de crear una nueva y más eficiente normativa procesal en dicho ámbito, a través del establecimiento de obligaciones para los proveedores de servicios que serían los destinatarios directos de la orden judicial. De esta forma, la idea pivotaba sobre la creación de una cooperación impuesta directamente a los proveedores de servicios como el principal objetivo de la Directiva[10].

La Directiva se traduce, en consecuencia, en el instrumento a través del cual se crea el marco legal que va a dotar de eficacia a la EPOC y a la EPOC-PR" (FRANSSEN, 2018). Y ello porque es en la Directiva donde se establece que los proveedores de servicios son los receptores directos de una orden emitida por un fiscal o por un juez –dependiendo de la naturaleza invasiva de la orden en la esfera de los derechos fundamentales de los usuarios afectados por la orden–. Una vez reciban dichas órdenes, pues, los proveedores quedan obligados a aportar los datos electrónicos que dicho órgano judicial requiera, así como, también (y en caso de ser necesario), adoptar las medidas necesarias para la conservación de datos que puedan resultar útiles a los efectos de una posterior EPOC, o incluso una OIE.

Evidentemente estamos ante la creación de un marco jurídico de deberes y obligaciones que conlleva medidas sancionadoras en caso de incumplimiento. En este sentido, por ejemplo, el artículo 5 de la Directiva ordena a los Estados miembros el establecimiento de un régimen de sanciones aplicable, que según el artículo 15 del Reglamento, podrá consistir en regular una sanción pecuniaria de hasta el 2% del total del volumen anual de negocios mundial del ejercicio precedente del prestador de servicios. Este tipo de sanciones de carácter disuasorio puede en algunos casos no ser eficaz si se tiene en cuenta, por ejemplo, que Google tuvo en el año 2022 un volumen de ingresos de casi 280 mil millones de dólares, los cinco mil seiscientos millones de dólares que debería pagar no va a suponer una cantidad excesiva, o al menos, tan disuasoria como se pretende.

El proveedor de servicios, por otro lado, podrá negarse a entregar los datos requeridos, pero únicamente por las razones y motivos expresamente recogidos en el artículo 12 del Reglamento[11]. Entre otros, por ejemplo, que los datos solicitados estén protegidos

9. ST9579/16.

10. Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo de 12 de julio de 2023. DOUE de 28 de julio de 2023.

11. Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023. DOUE de 28 de julio de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

por inmunidades o privilegios concedidos en virtud del Derecho del Estado de ejecución; o por normas sobre limitación de la responsabilidad penal relacionadas con la libertad de prensa; o porque existan motivos fundados para suponer que la ejecución de la orden supondría una vulneración manifiesta de un derecho fundamental de los recogidos en el artículo 6 del CEDH, y por ello, del derecho a un proceso justo, a la presunción de inocencia y al de defensa.

Se trata, tal y como se cita en el título de la Directiva, de establecer un marco normativo de armonización tanto de aquellas que impongan obligaciones, como de las que recojan sanciones por el no cumplimiento de lo solicitado en la orden, y que pueden imponerse a los proveedores de servicios con vínculos en la UE[12], lo que incluye a terceros países, como los EEUU (a través de los acuerdos bilaterales de los que se hacía mención en apartados anteriores esto es, el CLOUD Act) y que sirve para dejar sin efecto el denominado "Estatuto de Bloqueo", que no es otra cosa que la prohibición legal para los proveedores de servicios americanos de entregar datos electrónicos a otros estados no americanos y que se recoge en la ley *Electronic Communications Privacy Act* de 1986 (FRANSSSEN, 2018).

Y es que, el extraordinario incremento en la utilización –tanto por parte de los servicios de telecomunicaciones tradicionales, como de los consumidores y de las empresas– de los nuevos servicios basados en la red, –que hacen posible la comunicación interpersonal tales como servicios de voz sobre IP, mensajería instantánea de correo electrónico, junto a redes sociales como Facebook y Twitter–, permiten que los datos que compartan los usuarios estén cubiertos, de este modo, por la Directiva. Además, ha de tenerse en cuenta que cada vez resulta más común almacenar los datos en la nube, por lo que no es necesario que los proveedores de servicios tengan servidores en cada jurisdicción, ya que suelen utilizar sistemas centralizados para prestar sus servicios. Las transacciones que realizan las pueden llevar a cabo bien desde el sitio web del mercado en línea o en una página web del comerciante. Todas estas razones explican por qué era tan importante controlar y armonizar la normativa que impusiese obligaciones respecto de los proveedores de servicios, pues es este mercado precisamente el que suele estar en posesión de cualquier tipo de prueba electrónicas que sea necesaria obtener si se abre un proceso penal.

En este sentido, la Directiva es muy clara al señalar que, a los efectos de la obtención de pruebas electrónicas, los obligados a cooperar cuando se emita una orden de producción o de conservación son "los proveedores de servicios de comunicaciones electrónicas[13] y los prestadores de servicios de la sociedad de la información[14]". Respecto de

12. Con base jurídica en los artículos 53 y 62 del TFUE, que prevé la adopción de medidas de coordinación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de establecimiento y de prestación de servicios.

13. De esta forma, la Directiva debe aplicarse a los servicios de comunicación tal y como se definen en la Directiva (UE) 2018/1972 del Parlamento y del Consejo, de 11 de diciembre de 2018, por el que se establece el Código Europeo de las Comunicaciones Electrónicas.

14. Es decir, los prestadores de servicios de la sociedad de la información que puedan calificarse como tales según lo dispuesto en la Directiva (UE) 2015/1535 del Parlamento y del Consejo, de 9 de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

los primeros, la Directiva incluye las prestaciones de servicios de comunicaciones interpersonales tales como servicios de voz sobre IP, servicios de mensajería instantánea y servicios de correo electrónico. Y en relación con los servicios de la sociedad de la información, se refiere a los proveedores que ofrezcan la posibilidad de comunicación entre sujetos, o les ofrezcan servicios que puedan utilizar para almacenar o tratar datos de otro modo en su nombre, y que no puedan calificarse como proveedores de servicios de comunicación.

De esta forma se trata de proveedores que ofrecen servicios, en general, de comunicaciones electrónicas; así como de servicios de información, y de almacenamiento de datos como parte del servicio prestado al usuario, incluidas las redes sociales, los mercados en línea y otros proveedores de servicios de alojamiento de datos; y proveedores de servicios de asignación de nombres y números en internet (artículo 2 de la Directiva). Pero, habrá de tenerse en cuenta, también, que dichas obligaciones tienen implicaciones directas en otras empresas, tales como, por ejemplo, los fabricantes de automóviles que ofrezcan un servicio de navegación por la red o el acceso a emails, lo que resulta cada vez más común.

A los efectos de los obligados, y según el artículo 3 de la Directiva, los proveedores de servicios pueden dividirse, pues, en tres categorías principales: a) los que tengan su sede en un Estado miembro que ofrecen los servicios únicamente en el territorio de dicho Estado miembro; b) los que tengan su sede en un Estado miembro que ofrecen servicios en varios Estados miembros; y c) los que tengan su sede fuera de la UE pero que ofrecen sus servicios en uno o varios Estados miembros, dispongan o no de un establecimiento en uno o en varios Estados miembros. Así, la normativa contenida en la Directiva y en las correspondientes órdenes no sólo va a ser de aplicación a los servidores de servicios con sede en la UE, sino que, al recoger la exigencia de una conexión[15] vinculada a la oferta del servicio con efectos en el mismo ámbito geográfico, se impide una posible laguna legal que dificulte la ejecución de dichos instrumentos (TOSZA, 2020, p. 176). Esta última posibilidad resultará de vital importancia si tenemos en cuenta que los grandes proveedores de servicios, tales como Google y Microsoft, tienen su sede fuera de la UE.

En definitiva, la obligación de designar un establecimiento designado o un representante legal debe aplicarse a los prestadores que ofrezcan sus servicios en la Unión Europea, excluyéndose, a tales efectos, la aplicación de la Directiva a situaciones en las

septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.

15. Esta conexión a la que la Directiva llama "sustancial", se refiere, según el considerando número 11 de la Directiva, a la conexión del prestador de servicios "con la Unión. A falta de establecimiento, el criterio de la conexión sustancial debe basarse en criterios fácticos específicos como la existencia de un número significativo de usuarios en uno o más Estados miembros, o la orientación de las actividades hacia uno o más Estados miembros. La orientación de las actividades hacia uno o más Estados miembros ha de determinarse en función de todas las circunstancias pertinentes, incluidos factores como el uso de la lengua o una moneda utilizada generalmente en ese Estado miembro, o la posibilidad de encargar productos o servicios".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

que un prestador de servicios esté establecido en el territorio de un Estado miembro y ofrezca servicios exclusivamente en el territorio de dicho Estado.

III. Las órdenes europeas de entrega y conservación de pruebas electrónicas

Como se ha comentado anteriormente, el Consejo pidió la creación y desarrollo de acciones concretas basadas en un enfoque común de la UE para una asistencia jurídica mutua más eficaz, para mejorar la cooperación entre las autoridades de los Estados miembros y los proveedores de servicios radicados en países no pertenecientes a la UE, y encontrar soluciones al problema de la determinación y aplicación de la jurisdicción en el ciberespacio. Por su parte, el Parlamento Europeo también puso de relieve los retos que, el actualmente fragmentado marco jurídico, puede suponer para los proveedores de servicios que desean dar cumplimiento a los requerimientos legales, e hizo un llamamiento a favor del establecimiento de un marco jurídico europeo que incluyese salvaguardas para los derechos y las libertades de los interesados[16].

La opción de la Comisión por regular estas dos órdenes mediante Reglamento y no mediante Directiva o Decisión, según se declaró en la Exposición de Motivos de la Propuesta de Reglamento, se debía a que las órdenes van a ejecutarse en relación con procedimientos transfronterizos, y ello con buena lógica requiere de normas uniformes y, en consecuencia, la elaboración de un instrumento con forma de Reglamento es lo que va a permitir que, la misma obligación, sea impuesta de forma uniforme en cualquiera de los Estados miembros de la Unión.

La Exposición de Motivos de la Propuesta de Reglamento señalaba que la utilización de las redes sociales, los servicios de correo electrónico y de mensajería y las aplicaciones para comunicarse, trabajar, crear lazos sociales y obtener información se ha convertido en algo habitual en muchas partes del mundo. Estos servicios de mensajería instantánea (WhatsApp, Instagram, pero también e-mail, etc.), conectan entre sí a cientos de millones de usuarios y generan importantes beneficios para el bienestar social y económico de los usuarios en la Unión y fuera de ella. Sin embargo, también sirven como instrumentos para cometer o facilitar delitos de extrema gravedad, como, por ejemplo, atentados terroristas. Y, cuando esto sucede, los proveedores de servicios y las aplicaciones que ofrecen se convierten en el único lugar donde los investigadores pueden hallar indicios que les permitan determinar quién el presunto autor del hecho, y obtener las pruebas de cargo susceptibles de utilizarse en el proceso penal correspondiente.

Como es sabido, las redes sociales ofrecen servicios desde cualquier parte del mundo y a cualquiera que se encuentre en otra parte del mundo distinta, y todo ello sin

16. El fundamento jurídico para adoptar las medidas jurídicas correspondientes recogidas en el Reglamento se basó en el artículo 82, apartado 1 del TFUE, según el cual, podrán adoptarse las medidas que correspondan con arreglo al procedimiento ordinario a fin de establecer la normas y procedimientos que garanticen el reconocimiento en toda la Unión de las sentencias y resoluciones judiciales en todas sus formas.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

necesidad de una infraestructura física ni una presencia empresarial o personal en los Estados miembros en los que se ofrecen, o en el mercado interior en su conjunto. Por otro lado, y por su especial naturaleza, tampoco se requiere una ubicación específica para el almacenamiento de los datos, por lo que ésta suele ser elegida por el proveedor de servicios sobre la base de consideraciones tales como la seguridad de los datos, las economías de escala y la rapidez de acceso. Y, aquí radica la verdadera importancia de este instrumento jurídico: cada vez es más común que en los procesos penales, relativos a todo tipo de delitos, que las autoridades de los Estados miembros necesiten acceder a datos que puedan servir como prueba, pero que están almacenados fuera de su país, o por proveedores de servicios ubicados en otros Estados miembros o en terceros países.

El Reglamento aborda, pues, el problema específico derivado del carácter volátil de las pruebas electrónicas y su dimensión internacional. Es decir, con dicho instrumento se intenta adaptar los mecanismos de cooperación judicial a la era digital, ofreciendo a las autoridades judiciales y policiales las herramientas necesarias para abordar de forma eficaz el ámbito en el que los delincuentes se comunican en la actualidad, y, en consecuencia, enfrentarse de forma eficiente a la investigación de las nuevas formas de delincuencia.

De esta forma, el Reglamento tiene por objeto, por un lado, mejorar la seguridad jurídica para las autoridades, los proveedores de servicios y las personas afectadas, y, por otro lado, mantener un nivel uniforme en lo que respecta a las solicitudes de las autoridades competentes, y todo ello sin merma alguna de la debida protección de los derechos fundamentales, por lo que cualquier medida solicitada deberá estar informada y regida por el principio de necesidad y proporcionalidad[17].

Para la notificación y ejecución de órdenes en virtud de este instrumento, las autoridades deben recurrir al representante legal efectivamente designado por el proveedor de servicios. Se aporta así una solución común para todo el ámbito de la UE para transmitir órdenes a los proveedores de servicios por medio de un representante legal, que, según el artículo 3.7 del Reglamento, deberá ser una persona física o jurídica designada por escrito por un prestador de servicios no establecido en un Estado miembro que participe de un instrumento jurídico contemplado en el artículo 1, apartado 1[18] y en el artículo 3, apartado 1 de la Directiva[19].

17. Según se recoge expresamente en varios considerandos del Reglamento, tales como el 2 y el 49, así como en varios lugares de su articulado, como, por ejemplo, en el artículo 5 donde se establecen las condiciones de emisión de una EPOC.

18. Que dispone que la Directiva "establece las normas relativas a la designación de establecimientos designados y de representantes legales de determinados prestadores de servicios que ofrezcan servicios en la Unión para la recepción, el cumplimiento y la ejecución de las resoluciones y órdenes emitidas por las autoridades competentes de los Estados miembros a efectos de recabar pruebas electrónicas en procesos penales".

19. Según el cual, "Los Estados miembros velarán por que los prestadores de servicios que ofrezcan servicios en la Unión designen al menos un destinatario para la recepción, el cumplimiento y la ejecución de las resoluciones y órdenes que entren en el ámbito de aplicación establecido en el artículo 1, apartado 2 (en lo sucesivo 'resoluciones y órdenes comprendidas en el ámbito de aplicación

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

En relación con las infracciones susceptibles de ser objeto de una EPOC, el artículo 5 del Reglamento establece que podrá emitirse para cualquier infracción punible en el Estado emisor con una pena máxima de privación de libertad de al menos tres años; o bien cuando las infracciones se hayan cometido en su totalidad, o parcialmente, por medio de un sistema de información respecto de las infracciones que, como tal, se definen en: a) la Directiva (UE) 2019/713 del parlamento y del Consejo sobre la lucha contra el fraude y la falsificación de medios de pago distintos al efectivo por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo (transferencias fraudulentas, robo o apropiación indebida de instrumentos de pago, etc.); b) infracciones como las recogidas en la Directiva 2011/93/UE del Parlamento Europeo y del Consejo (relativas a los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, que sustituye la Decisión Marco 2004/68/JAI del Consejo); c) las infracciones recogidas en la Directiva 2013/40/UE del Parlamento Europeo y del Consejo (relativa a los ataques contra los sistemas de información, que sustituye a la Decisión Marco 2005/222/JAI del Consejo); y d) las infracciones recogidas en la Directiva 2017/541 del Parlamento Europeo y del Consejo (relativa a la lucha contra el terrorismo, que sustituye la Decisión Marco 2005/671/JAI del Consejo).

3.1. Tipo de datos que pueden obtenerse como prueba electrónica

En relación con el tipo de datos que pueden obtenerse a través de una EPO o EPOC-PR, ha de tenerse en cuenta que el Reglamento regula únicamente la obtención de datos almacenados por un prestador de servicios en el momento que reciba una orden europea de producción o de conservación. De esta forma, no podrán realizarse investigaciones prospectivas con la intención de obtener datos pasados o futuros. Los datos deberán facilitarse o conservarse independientemente de que estén cifrados o no, y deberá existir una previa imputación en relación con un delito concreto y, en consecuencia, que exista un proceso penal abierto en el momento en el que se soliciten.

Por otro lado, es importante señalar que el Reglamento no define expresamente qué debe entenderse por prueba electrónica, sino que simplemente hace referencia a la clase de datos objeto de la Orden, y en este sentido ha de entenderse que prueba electrónica es "la evidencia almacenada en forma electrónica por o a nombre de un proveedor de servicios en el momento de la recepción de la orden y consistente en una de las cuatro categorías tradicionales de datos: datos de abonado, de acceso, de tráfico y de contenido"[20]. Estas categorías son, en efecto, las que se recogen en el artículo 3

establecido en el artículo 1, apartado 2'), emitidas por las autoridades competentes de los Estados miembro a efectos de recabar pruebas en procesos penales".

20. Según el Informe de la propuesta de regulación publicado por el Parlamento Europeo, en la enmienda núm. 20, se justifica la cobertura de los tipos de datos mencionados por ser las categorías más comunes en muchos de los Estados miembros y en la normativa de la Unión, como la Directiva 2002/58/EC, la jurisprudencia del Tribunal de Justicia, y por supuesto, el Convenio del Cibercrimen. Vide https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

(núm. 9 a 11), de forma que el Reglamento coloca el énfasis en lo que TOSZA denomina "objeto de la Orden", en vez de focalizarlo en la naturaleza jurídica de lo debe entenderse por "prueba electrónica" (TOSZA, 2020, p. 171 y LARO, 2022, p. 291).

En este sentido, en la Propuesta se aseguró que en el Reglamento se recogiese un concepto de datos coherente con los establecidos en otros instrumentos europeos en relación con las comunicaciones electrónicas y, en especial, con lo contenido en el Código Europeo de Comunicaciones Electrónicas creado por la Directiva de 11 de diciembre de 2018[21]. Sin embargo, como señala ROGALSKI, el concepto de lo que ha de entenderse por "abonado" no lo encontramos en la Directiva que acaba de mencionarse, sino en el artículo 2, letra k de la Directiva 2002/21/EC del Parlamento y del Consejo de 7 de marzo de 2002, que fue reemplazada por la anterior, y que definía el termino de abonado como "cualquier persona física o jurídica que haya celebrado un contrato con un proveedor de servicios de comunicaciones electrónicas disponibles para el público para la prestación de dichos servicios". Y en este aspecto, es claro que, como señala el citado autor, es importante que, en relación con el tipo de datos que son susceptibles de ser obtenidos y/o conservados, los significados deben ser uniformes en los distintos códigos procesales penales de los Estados miembros (ROGALSKI 2020, pp. 340-341).

En opinión de CORTHAY, sin embargo, el Reglamento se separa de las categorías tradicionales de datos que suele utilizar la Comisión en otros instrumentos jurídicos, por ejemplo, en la Directiva 2002/58/CE del Parlamento y del Consejo de 12 de julio, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, más conocida como la Directiva e-Privacy; y la Directiva 2006/24/CE de Conservación de datos[22] que modifica la anterior. En estos instrumentos se utilizan las categorías de datos de abonado, datos de tráfico y de localización (conocidos como metadatos) y de contenido (CORHAY, 2021, p. 447). Pero el Parlamento rechazó las categorías de datos propuestas por la Comisión, y optó por mantener las categorías tradicionales de datos: de abonado, de tráfico y de contenido (CORHAY, 2021, p. 458).

Así pues, los tipos de datos que recoge el Reglamento son los siguientes:

a) *Datos de los abonados*
   El Reglamento considera datos de los abonados cualquier dato que obre en poder de un prestador de servicios relativo a la suscripción da sus servicios en relación con la identidad del abonado o cliente, como el nombre, fecha de nacimiento, dirección postal o geográfica, facturación y pagos, número de teléfono o dirección de correo electrónico.

21. Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo de 11 de diciembre de 2019 por la que se establece el Código Europeo de las Comunicaciones Electrónicas (DOUE de 17 de diciembre de 2018).

22. Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso o redes públicas de comunicaciones por la que se modifica la Directiva 2002/58/CE (DOUE núm. 105, de 13 de abril de 2006.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

Y, además de estos, se incluye: el tipo de servicio y su duración, incluidos los datos técnicos que identifiquen las medidas técnicas correspondientes o las interfaces utilizadas o facilitadas al abonado o cliente en el momento del registro o activación inicial, y los datos relativos a la validación del uso del servicio, excluyendo las contraseñas u otros medios de autenticación utilizados en lugar de una contraseña que hayan sido facilitados por un usuario o creados a petición de un usuario.

b) *Datos de identificación del usuario (datos de acceso)*
Tales como las direcciones de IP, los números de acceso y la información conexa. Estos datos pueden constituir un punto de partida esencial para las investigaciones en las que no se conozca la identidad de un sospechoso. Son datos que forman parte de un registro de acontecimientos conocido como registro de servidor que indica el comienzo o fin de la sesión de acceso de un usuario a un servicio. A menudo es una dirección IP (estática o dinámica[23]) y otro identificador el que señala la interfaz de red utilizada durante una sesión de acceso de un usuario a un servicio como los puertos de origen y sello de tiempo, ya que las direcciones de IP suelen compartirse entre usuarios, por ejemplo, cuando se dispone de una traducción de direcciones de redes de alta fiabilidad (CGN), o de equivalentes técnicos. Se trata de un conjunto de mecanismos dirigido a compartir dirección IP entre varios dispositivos. El ejemplo más claro son las conexiones de banda ancha de suscriptores. El proveedor asigna una sola dirección IP a un suscriptor y mediante un dispositivo con capacidades NAT se realiza la traducción del conjunto de direcciones privadas utilizadas en el domicilio del suscriptor, contra la única dirección IP que el proveedor ha asignado al abonado (CASTRO, 2020, p. 5).

Las direcciones de IP dinámicas de acuerdo con la jurisprudencia de la UE deben considerarse datos personales y gozar de plena protección en virtud de materia de protección de datos[24]. Pero, en determinadas circunstancias, las direcciones de IP pueden también considerarse datos de tráfico, por ejemplo, los números de acceso y la información conexa se consideran datos de tráfico en algunos Estados miembros. No obstante, a efectos de una investigación penal específica, las autoridades policiales pueden solicitar una dirección de IP, así como números de acceso e información conexa con el único fin de identificar al usuario antes de que puedan solicitarse al prestador de servicios los datos de los abonados relacionados con ese identificador en tal caso, procede aplicar el mismo régimen que a los datos de los abonados. En este ámbito, sin embargo, y a raíz de una solicitud de la Gran Sala, presentada como cuestión prejudicial planteada por el Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo de Francia, las conclusiones del Abogado General

23. Mientras que las IP estáticas no cambian cuando se asigna a un dispositivo, las dinámicas tienen carácter personal, y cambia con cada nueva conexión a internet, ya que son las que les asigna la red cuando se conectan.

24. Así se estableció en el caso C582/14 Breyer.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

Maciej Szpunar, en el asunto C-470/21, de 23 de marzo de 2023, declaró que una autoridad nacional debería poder acceder a los datos de identidad civil vinculados a las direcciones IP cuando dichos datos constituyen el único método de investigación para identificar a los titulares de esas direcciones sospechosos de vulnerar derechos de propiedad intelectual[25].

c) *Datos de tráfico*

Son los datos relacionados con la prestación de un servicio que sirvan para facilitar información contextual o adicional sobre dicho servicio y sean generados o tratados por un sistema de información contextual o adicional sobre dicho servicio y sean generados o tratados por un sistema de información del prestador del servicio tales como el origen y destino de un mensaje u otro tipo de interacción, el número de teléfono móvil, la ubicación del dispositivo, la fecha, la hora, la duración, el tamaño, la ruta, el formato, el protocolo utilizado y el tipo de compresión, y otros metadatos de las comunicaciones electrónicas y los datos que no sean datos de abonados, relativos al inicio y final de una sesión de acceso del usuario a un servicio, tales como la fecha y hora del acceso, la conexión y desconexión del servicio.

d) *Datos de contenido*

Cualquier dato en formato digital, como texto, voz, videos, imágenes y sonidos que no sean datos de abonados o datos de tráfico.

3.2. Autoridad competente para la obtención y solicitud de conservación de prueba electrónica

Una de las cuestiones más controvertidas y por ello más debatidas por la doctrina tras la publicación de la Propuesta del Reglamento ha sido la cuestión acerca de la determinación de la autoridad competente para emitir tanto una orden de obtención como de conservación de pruebas electrónicas. Y ello porque la Propuesta autorizaba tanto a un órgano judicial, como a un miembro de la Fiscalía, a emitir cualquiera de las órdenes previstas sin diferenciar el tipo de datos y, en consecuencia, de la distinta afectación a los derechos fundamentales del propietario de dichos datos.

En este sentido, el Dictamen del Comité Económico Social Europeo[26] (CESE) señalaba que el Reglamento debía respetar los derechos fundamentales, tanto en relación con los recogidos y reconocidos en el CEDH, como todos los reconocidos en las Constituciones de cada uno de los Estados miembros; en especial, el derecho a la libertad y seguridad, el derecho a la tutela judicial efectiva, y el de protección de los datos de carácter personal.

25. https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-10/cp220172es.pdf

26. Dictamen publicado en el Diario Oficial de la Unión Europea de 10 de octubre de 2018 C 367/88. El Comité Económico y Social Europeo, es el órgano consultivo de la UE, compuesto por los representantes de las organizaciones de trabajadores y empresarios, y que emite dictámenes sobre cuestiones de la UE para la Comisión Europea, el Consejo y el Parlamento Europeo, y actúa como puente entre las instituciones de la UE con capacidad decisoria y los ciudadanos europeos

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

En dicho aspecto, el CESE consideraba que tanto la solicitud de obtención de datos de abonados como la de datos relativos al acceso pertenecen al ámbito de los derechos de carácter personal, por lo que la orden debería estar acordada y emitida por una autoridad judicial y no por un fiscal.

Por su parte, el Supervisor Europeo de la Protección de Datos[27] (EDPS, por sus siglas en inglés), publicada el 6 de noviembre de 2019 como "Opinión 7/2019 sobre la Propuesta de Reglamento de la Orden Europea de obtención y conservación de pruebas electrónicas"[28], realizó recomendaciones dirigidas, por un lado, a que la normativa europea fuese clara y se reforzase la seguridad jurídica, y por otro, que el principio de proporcionalidad se aplicase en el listado de las infracciones susceptibles de ser objeto de una orden (de obtención o de preservación de pruebas).

De esta forma, el EDPS entendía que el límite de tres años de privación de libertad –que recoge el vigente el artículo 5 (4) (a-d) del Reglamento– implicaría que podría solicitarse una orden de este tipo para casi cualquier delito recogido, como tal, en las normativas penales de los Estados miembros, y que podía servir de coladero para otros delitos no recogidos en el listado –anteriormente mencionado–. En dicho aspecto, recordaba que el TJUE, en su decisión C-207/16, ya declaró que "de acuerdo con el principio de proporcionalidad, las graves interferencias por parte del Estado en áreas de la prevención, investigación, detección y persecución penal, sólo puede estar justificado si el delito que se ha cometido puede ser definido como grave, y, únicamente cuando la lucha contra dicha grave criminalidad posibilite justificar al Estado el acceso a datos personales, permitiéndole obtener información relativa a la privacidad de las personas cuyos datos han sido obtenidos". Por otro lado, la exigencia de garantizar la protección a los derechos fundamentales, y en especial, a los datos de carácter personal, es un objetivo esencial. Por ello, las órdenes deberán, en cualquier caso, ser emitidas por una autoridad judicial, no por un fiscal.

En su informe de 2020, investigadores del Centro de Estudios Europeos, insistieron en la necesidad de una validación judicial independiente de las órdenes de obtención y conservación de pruebas digitales y siempre bajo los principios de legalidad, necesidad y proporcionalidad. (Sergio Carrera, M. S. y. V. M., 2020).

Finalmente, en mayo de 2023, pocos meses antes de la publicación de los instrumentos que se están analizando, el European Law Institute, hizo pública una Propuesta de Regulación de la Admisibilidad Mutua de Prueba y Prueba electrónica en los procesos penales dentro de la Unión Europea, en la que recomienda la regulación positiva

27. El EDPS es una institución independiente de la UE y responsable, bajo el artículo 52.2 del Reglamento 2018/1725 de los procesos relacionados con los datos personales para asegurar que los derechos y libertades fundamentales, en particular el derecho fundamental a la protección de datos personales y, bajo el artículo 52.3, para aconsejar a las instituciones de la Unión, así como emitir, por propia iniciativa o, tras la previa solicitud de las instituciones de la Unión, en relación con la protección de datos personales. Vide edps.europa.eu.

28. EDPS Opinion on the Proposals regarding European Production and Preservation Orders of electronic evidence on criminal maters. https://edps.europa.eu/sites/edp/files/publication/opinion_on_e_evidence_proposals_en.pdf

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

de ciertos aspectos importantes, - aunque no todos ellos se han recogidos en el vigente Reglamento–, tales como la inclusión de salvaguardas dirigidas a evitar manipulaciones o alteraciones de la integridad y autenticidad de las pruebas electrónicas mediante la posibilidad de que la defensa tenga acceso a todo el material obtenido, y el uso de recursos frente a la obtención de pruebas con infracción de las normas y la regulación de las consecuencias de la declaración de ilicitud de la obtención de pruebas mediante el establecimiento de criterios de inadmisibilidad (MARTINEZ, 2023, p. 11).

Tras todas las consideraciones anteriores, lo cierto es que el Reglamento, en su considerando 10, haciéndose eco de las previas advertencias, reconoce que en el mismo se observa el respeto por los derechos fundamentales y los principios reconocidos en el artículo 6 del CEDH y de los Tratados Internacionales para la Protección de Derechos Humanos, incluyendo el derecho a la libertad y a la seguridad, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la libertad de empresa, el derecho a la propiedad, a la tutela judicial efectiva y a un juez imparcial, la presunción de inocencia, el derecho de defensa, y los principios de legalidad y proporcionalidad. Y en su considerando 17, declara que, a fin de garantizar el pleno respeto de los derechos fundamentales, el valor probatorio de las pruebas obtenidas en aplicación del Reglamento deberá ser valorado por un juez competente de conformidad con el Derecho nacional, cuestión esta que era imaginable dada la reticencia del TEDH a establecer una doctrina respecto a cuando debe o no excluirse una prueba por vulnerar el derecho al debido proceso.

De esta forma, al menos el texto final –en relación con la Propuesta inicial– parece haber mejorado mucho al recoger la mayoría de las recomendaciones de los organismos y de la doctrina en relación con las modificaciones que necesitaban operarse en lo que la Propuesta inicialmente contenía.

Así, el artículo 4 del Reglamento, al regular la autoridad emisora, tanto del EPOC, como de la EPOC-PR, señala claramente que la obtención de datos de abonados y de acceso sólo podrán ser recabados por un juez o fiscal competente; y la de datos de tráfico (excepto para obtener datos solicitados con el único fin de identificar al usuario) y de contenido solo podrán ser recabados por un órgano judicial.

Sin embargo, cuando se trata de solicitar la conservación de datos de cualquier tipo, podrá emitirse una orden por un juez, un fiscal o cualquier otra autoridad competente que actúe como investigador en los procesos penales, lo que incluye a los cuerpos y fuerzas de seguridad del Estado. En este último caso, no obstante, la orden deberá ser validada previo examen de su conformidad con las condiciones del Reglamento por un juez o fiscal. En casos de urgencia[29], la policía, o el fiscal podrá solicitar la obtención de

29. Entendiendo por "caso urgente", según el artículo 3.18 del Reglamento, "la situación en la que exista una amenaza inminente para la vida, la integridad física o la seguridad de una persona o para una infraestructura esencial, tal y como se define en el artículo 2, letra a) de la Directiva 2008/114/CE, cuando la perturbación o destrucción de dicha estructura esencial pueda dar lugar a una amenaza inminente para la vida, integridad física o la seguridad de una persona, también mediante perjuicios graves al suministro de productos básicos para la población o para el ejercicio de las funciones esenciales del Estado".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

datos de abonado, con la finalidad de poder identificar al sospechoso sin una previa autorización judicial, pero, ésta deberá emitirse como máximo 48 horas después de la emisión de la orden.

De esta forma, en el proceso de emisión o validación de una orden europea siempre debe intervenir una autoridad judicial. Habida cuenta del carácter especialmente sensible de los datos de tráfico, excepto en el caso de los datos solicitados con el único fin de identificar al usuario, tal y como se definen en el Reglamento, y de los datos de contenido, la emisión o validación de una orden europea de producción para obtener esas categorías de datos requiere el control de un juez. Puesto que los datos de los abonados y los datos solicitados con el único fin de identificar al usuario; tal y como se definen en el Reglamento, son de carácter menos sensible, una orden europea de producción para obtener dichos datos también puede ser emitida o validada por un fiscal competente.

En cuanto a la emisión, la orden se envía al representante legal elegido por el proveedor de servicios y debe tener la forma de certificado, tal y como se señala en el artículo 9 del Reglamento. El certificado es un formulario estandarizado que deberá contener la información a la que se refiere el artículo 5.5 (a-j)[30]. Hay que diferenciar pues, entre la orden y el certificado, puesto que mientras el certificado no exige motivación, la orden sí debiendo ser escrupulosa y razonada en relación con el principio de necesidad y proporcionalidad (TOSZA, 2020, p. 174).

Por último, y respecto del plazo para la preservación de los datos, el Reglamento establece un máximo de 60 días, pero, si se notifica que va a emitirse una orden de obtención de datos (o una OIE), este plazo podrá prorrogarse hasta que se haya emitido la orden correspondiente. En este sentido poco ha cambiado el texto de la Propuesta con el del Reglamento vigente. Ya se criticaba, y con razón, que los datos pueden llegar a estar conservados "el tiempo que sea necesario" (artículo 11.2), lo que en la práctica puede generar problemas en relación con los derechos de los usuarios, de forma que debería haberse establecido un periodo de tiempo limitado para la eliminación de los datos en caso de no solicitase su entrega a la autoridad competente (ROGALSKI, 2020, p. 349).

30. Una orden europea de producción incluirá la información siguiente: (a) la autoridad emisora y, cuando proceda, la autoridad validadora; b) el destinatario de la orden europea de producción a que se refiere el artículo 7; c) el usuario, excepto cuando la única finalidad de la orden sea identificar al usuario, o cualquier otro identificador único como el nombre de usuario, el identificador de inicio de sesión o el nombre de la cuenta a fin de determinar los datos solicitados; d) la categoría de los datos solicitados tal como se definen en el artículo 3, puntos 9 a 12; f) en su caso, el período de tiempo que cubren los datos cuya producción se solicita; g) las disposiciones de Derecho penal aplicables del Estado emisor; en casos urgentes, tales como se definen en el artículo 3, punto 18, las razones debidamente justificadas de la urgencia; h) en los casos en que la orden europea de producción se dirija directamente al prestador de servicios que almacene o trate datos de otro modo en nombre del responsable del tratamiento, una confirmación de que se cumplen las condiciones establecidas en el apartado 6 del presente artículo; i) los motivos para determinar que la orden europea de producción cumple las condiciones de necesidad y proporcionalidad establecidas en el apartado 2; y j) una descripción sucinta del caso.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

3.3. Recursos frente a la Orden Europea de Producción y valoración de la prueba obtenida

El Reglamento recoge, en su artículo 18, la posibilidad de que la persona cuyos datos se hayan solicitado mediante la emisión de una EPOC tendrá la posibilidad de recurrirla. En caso de tratarse del sospechoso o acusado, tendrá derecho a la utilización de vías efectivas de recurso durante la tramitación del proceso penal en el que se estén utilizando los datos.

Este recurso se interpondrá ante el órgano jurisdiccional del Estado emisor y seguirá los cauces establecidos para ello en su Derecho nacional, pero deberá incluir la posibilidad de impugnar la legalidad, la necesidad y la proporcionalidad de la medida. Sin embargo, como De HOYOS entiende muy certeramente, el que los recursos deban solicitarse en el país del Estado emisor de la orden "puede dificultar el ejercicio del derecho de defensa de los afectados cuando sean residentes en el Estado de ejecución" (De HOYOS, 2023, p. 108).

En el apartado 5 del artículo 18, además, se recoge la exigencia de que se respeten los derechos de defensa y equidad del proceso en la valoración de las pruebas obtenidas a través de la orden europea de producción. En este sentido, una vez más, se deja en manos de la normativa nacional la decisión acerca de cuándo debe excluirse una prueba por entenderse obtenida vulnerando derechos fundamentales, cuestión que, como se sabe, no goza de un criterio uniforme en el ámbito de la UE, ni de la doctrina del TEDH.

IV. Conclusiones

Los recientemente promulgados instrumentos europeos con forma de Directiva y de Reglamento, conteniendo las órdenes de producción y de conservación de pruebas electrónicas han introducido, en el ámbito del proceso penal y de la obtención de pruebas electrónicas transfronterizas, una solución inédita y potencialmente más efectiva y eficaz que los variados instrumentos provenientes del Parlamento y la Comisión conocidos hasta el momento.

Y es que, el extraordinario incremento en la utilización –tanto por parte de los servicios de telecomunicaciones tradicionales, como de los consumidores y de las empresas– de los nuevos servicios basados en la red, –que hacen posible la comunicación interpersonal tales como servicios de voz sobre IP, mensajería instantánea de correo electrónico, junto a redes sociales como Facebook y Twitter–, permiten que los datos que compartan los usuarios estén cubiertos, de este modo, por la Directiva. Además, ha de tenerse en cuenta que cada vez resulta más común almacenar los datos en la nube, por lo que no es necesario que los proveedores de servicios tengan servidores en cada jurisdicción, ya que suelen utilizar sistemas centralizados para prestar sus servicios. Las transacciones que realizan las pueden llevar a cabo bien desde el sitio web del mercado en línea o en una página web del comerciante. Todas estas razones explican por qué

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

era tan importante controlar y armonizar la normativa que impusiese obligaciones respecto de los proveedores de servicios, pues es este mercado precisamente el que suele estar en posesión de cualquier tipo de prueba electrónicas que sea necesaria obtener si se abre un proceso penal.

La valoración respecto de la anterior propuesta –en la que no se diferenciaba el tipo de datos y la injerencia en los derechos fundamentales del usuario–, es muy positiva, puesto que, en el vigente Reglamento tanto el proceso de emisión como el de validación de una orden europea queda cubierto por la intervención de una autoridad judicial. Habida cuenta del carácter especialmente sensible de los datos de tráfico, excepto en el caso de los datos solicitados con el único fin de identificar al usuario, tal y como se definen en el Reglamento, y de los datos de contenido, la emisión o validación de una orden europea de producción para obtener esas categorías de datos requiere el control de un juez. Sin embargo, existen otras cuestiones que no alcanzan una valoración tan positiva.

En relación con el valor probatorio de lo obtenido, por ejemplo, y a fin de garantizar el pleno respeto de los derechos fundamentales, se establece que deberá ser valorado por un juez competente de conformidad con el Derecho nacional, y esta cuestión podría haberse resuelto de una vez, estableciendo una normativa uniforme respecto de cuando debe o no excluirse una prueba por vulnerar el derecho al debido proceso, simplemente declarando que la prueba obtenida en circunstancias de urgencia sin el aval posterior de un órgano judicial, por ejemplo, no podrá utilizarse como prueba en ningún tipo de procesos. Por otro lado, también hubiese sido deseable poner un límite temporal al plazo para conservar los datos electrónicos por parte de los proveedores de servicio solicitados. El uso de prórrogas para terminar permitiendo que podrán conservarse los datos "el tiempo que sea necesario" puede generar problemas procesales, pues parece contradecir la prohibición de que dichos datos estén disponibles en el momento de la solicitud de una orden judicial, siempre que exista un proceso penal abierto. Y ello parece que no casar bien con la posibilidad de solicitar la conservación y aseguramiento de una prueba por tiempo indefinido.

Bibliografía

CASTRO SÁNCHEZ, A. (2020). Propuesta de implementación de Carrier-Grade NAT para Guifi.net. Uoc.edu. https://openaccess.uoc.edu/bitstream/10609/118086/7/aaroncastroTFM-0620memoria.pdf

CORHAY, M. (2021). Private Life, personal Data Protection and the Role of Service Providers: The EU E-Evidence Proposal. European Papers, 6.

DE HOYOS SANCHO, M. (2023). Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo". Revista de Estudios Europeos Nº Extraordinario monográfico, *1*.

FRANSSEN, V. (2018). *The European Commission's E-evidence proposal: Toward an EU-wide obligation for service providers to cooperate with law enforcement?* European Law Blog. https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06

LARO GONZÁLEZ, E. (2022). Prueba penal transfronteriza: de la orden europea de investigación a las órdenes europeas de entrega y conservación de pruebas electrónicas". Revista de Estudios Europeos, 79.

MARTÍNEZ SANTOS, A. (2023). Admisibilidad mutua de prueba penal transfronteriza en la Unión Europea: La propuesta de Directiva del European Law Institute", en Revista General del Derecho Procesal.

PEERS, S. (2023). *"The proposed European Investigation Order: Assault on human rights and national sovereignty"*, http://www.statewatch.org/analyses/no-96-european-investigation-order.pdf

ROGALSKY, M. (2020). The European commission's e-evidence proposal –critical remarks and proposal for changes. European Jouranl of Crime Criminal Law and Criminal Justice 28(4), 333-353, https://doi.org/10.1163/15718174-bja10018

SAYERS, D. (2011). "*The European Investigation Order. Traveling without a 'roadmap*". En www.ceps.eu.

SERGIO CARRERA, M. S. y. V. M. (2020). *Cross-Border Data Acces in Criminal Proceedings and the Future of Digital Justice. Centre for European Policy Studies* (CEPS). https://www.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf

TOSZA, S. (2020). "*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 la*

Documentos

Conclusiones del Consejo de la Unión Europea, de 9 de junio de 2016, sobre la mejora de la justicia penal en el ciberespacio, ST9579/16.

Dictamen publicado en el Diario Oficial de la Unión Europea de 10 de octubre de 2018 C 367/88

EDPS Opinion on the Proposals regarding European Production and Preservation Orders of electronic evidence on criminal maters. https://edps.europa.eu/sites/edp/files/publication/opinion_on_e_evidence_proposals_en.pdf

Fair Trials International "Fair Trials International's response to a European Member States's legislative initiative for a Directive on a European Investigation Order", de 29 de junio de 2010, http://www.statewatch.org/news/2010/jul/eu-eio-ft-briefing.pdf.

Recomendación para la autorización de negociaciones con vistas a un acuerdo entre la Unión y los EEUU de América sobre acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en asuntos penales, de 5 de febrero de 2019 COM (2019) 70 final.https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf

Recomendación para una decisión del Consejo sobre la autorización a participar en las negociaciones de un segundo Protocolo Adicional del Convenio Europeo sobre Cibercrimen (CETS No 185). De 5 de febrero de 2019 COM (2019) 71 final. https://ec.europa.eu/info/sites/info/files/recommendation_budapest_convention.pdf

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 117-135
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.06