

E-evidence: ¿una evidencia?

E-evidence: an evidence?

Anna VILÀ CUÑAT

Profesora asociada e investigadora en Derecho Penal

Universitat Autònoma de Barcelona (España)

Anna.Vila.Cunat@uab.cat

<https://doi.org/10.14201/rspc.31480>

Artículo original sin previa publicación

Fecha de recepción: 28/02/2023

Fecha de aceptación: 19/04/2023

Resumen

Este artículo analiza críticamente los puntos clave de la propuesta de Reglamento Europeo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas en materia penal. El texto presenta puntos en común con otros mecanismos de cooperación judicial, como el sustento en la confianza mutua. Sin embargo, da un paso más allá en el proceso de ejecución de las órdenes emitidas y la configuración de las mismas. El mecanismo

Abstract

This article critically analyzes the key points of the proposal for a European Regulation on European orders for the production and preservation of electronic evidence in criminal matters. The text has points in common with other judicial cooperation mechanisms, such as its reliance on mutual trust. However, it goes a step further in the process of executing the orders issued and their configuration. The mechanism echoes

se hace eco del tenso debate entre eficacia procesal y garantías de los procesados.

the tense debate between procedural efficiency and guarantees for defendants.

Palabras clave: Cooperación judicial; Prueba electrónica; Confianza mutua; Protección de datos; Ciberseguridad.

Keywords: Judicial cooperation; Electronic evidence; Mutual trust; Data protection; Cybersecurity.

Sumario: 1. Consideraciones preliminares. 2. La búsqueda de la eficacia procesal. 2.1. Un actor privado legitimado. 2.2. Una evaluación parcialmente neutralizada. 3. La injerencia en los derechos fundamentales. 3.1. Una protección mermada de los datos personales. 3.2. Una intromisión progresivamente normalizada. 4. Conclusiones. 5. Referencias.

1. CONSIDERACIONES PRELIMINARES

Conscientes del importante lugar que ocupan las tecnologías de la comunicación en nuestra sociedad y habiendo constatado que los delincuentes utilizan a escala transnacional dispositivos electrónicos cada vez más sofisticados, las autoridades europeas han empezado a desarrollar herramientas destinadas a facilitar y agilizar la obtención de pruebas electrónicas por parte de autoridades policiales y judiciales. La propuesta de Reglamento relativa a las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, presentada por la Comisión Europea, el 17 de abril de 2018¹ (en adelante, “la propuesta”), singulariza e individualiza la prueba de naturaleza electrónica, erigiéndola en una categoría independiente y diferenciada del régimen que actualmente regula la orden europea de investigación.

En esta fase introductoria, debemos centrar nuestra atención en la elección del instrumento utilizado para la regulación. Cabe destacar en este sentido que la mayoría de los textos europeos en materia penal están recogidos en decisiones marco o directivas, por lo que los Estados miembros conservan cierto margen de maniobra en la operación de transposición. Sin embargo, la propuesta aquí estudiada se presenta en forma de reglamento, algo que refleja el deseo de imponer normas uniformes a todos los Estados miembros, sin riesgo de disparidades ni retrasos en la transposición². La base jurídica del reglamento es el artículo 82, apartado 1, del Tratado de Funcionamiento de la Unión Europea (UE), que dispone que podrán adoptarse medidas con arreglo al procedimiento

1. 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 COM/2018/225 final - 2018/0108 (COD).

2. Así lo reconoce la exposición de motivos de la propuesta estudiada (apartado “elección del instrumento”, en 2. Base jurídica, subsidiariedad y proporcionalidad).

legislativo ordinario para establecer normas y procedimientos para garantizar el reconocimiento en toda la Unión de las sentencias y resoluciones judiciales en todas sus formas. El uso del reglamento en el caso aquí estudiado conlleva, por lo tanto, consecuencias a dos niveles. Pese a ser este instrumento directamente aplicable y obligatorio en todos sus elementos, fija normas de procedimiento y establece garantías para los derechos y las libertades de los interesados, creando un marco general para la cooperación, sin armonizar normas nacionales, a diferencia de la Directiva sobre la designación de un representante legal del prestador, que sí lo hace³. De esta manera, el Reglamento sobre la prueba electrónica, basado en el apartado 1 del artículo 82, hace de esta propuesta un instrumento de cooperación judicial al servicio del principio de reconocimiento mutuo⁴.

Así pues, estudiaremos aquí otro texto más que se añade al “cajón de sastre” de los instrumentos de cooperación penal de carácter operativo que conforman el Espacio de Libertad, Seguridad y Justicia.

En el curso de este trabajo, que, dado la novedad del tema que aborda, se centra en el análisis de la normativa de las instituciones europeas en materia de *e-evidence*, buscaremos determinar hasta qué punto la propuesta de Reglamento logra un equilibrio entre los derechos y garantías fundamentales y la eficacia procesal.

Consideramos que la propuesta de Reglamento sobre la prueba electrónica tiende a la búsqueda de la eficacia en las investigaciones judiciales (2), a costa de una protección de los derechos fundamentales que se ve menoscabada (3).

2. LA BÚSQUEDA DE LA EFICACIA PROCESAL

La orden europea de investigación (en adelante, “OEI”)⁵ y la orden de detención europea (en adelante, “ODE”)⁶ constituyen conjuntamente los dos instrumentos predominantes de asistencia judicial entre los Estados miembros. Especialmente en un

3. La propuesta de Reglamento va acompañada de una propuesta de Directiva 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 2018/0107(COD), que no será tratada frontalmente en este trabajo.

4. Para una crítica del uso de este fundamento en el ámbito de la obtención transfronteriza de pruebas, vid. AMBOS, Kai. 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 Llorente Sánchez-Arjona, Mercedes (Dir.). *Estudios procesales sobre el espacio europeo de justicia penal*. Cizur Menor: Aranzadi, 2021.

5. Directiva 2014/41/CE del Parlamento Europeo y del Consejo de 3 de abril de 2014 relativa a la orden europea de investigación en materia penal.

6. Decisión Marco del Consejo 2002/584/JAI de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros.

contexto en el que se cuestiona el Estado de Derecho⁷, la contienda jurídica que, veinte años después de su instauración sigue protagonizando la ODE, muestra la fragilidad del principio de confianza mutua, lo que constituye, a su vez, la base de los mecanismos de reconocimiento entre los Estados miembros.

Pese a ello, en el caso que aquí nos ocupa, se parte de un supuesto nivel de confianza intensificado. Ello tendrá implicaciones tanto en la configuración del nuevo mecanismo propuesto (2.1), como en el contenido de sus disposiciones (2.2).

2.1. *Un actor privado legitimado*

La propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal establece que la autoridad emisora, normalmente un juez, dirigirá la orden europea de entrega (EPOC) y la orden europea de conservación (EPOC-PR) directamente a un representante legal designado por el proveedor de servicios con el fin de recabar pruebas en un proceso penal. Si no se ha designado a un representante legal concreto, las órdenes podrán ser dirigidas a cualquier establecimiento del prestador de servicios en la Unión⁸. Las nuevas órdenes permiten de esta manera obtener o conservar pruebas electrónicas independientemente del lugar donde se encuentren los datos.

Para ello, la propuesta exige como base y requisito previo para su correcto funcionamiento “un alto nivel de confianza mutua entre los Estados miembros”⁹. La confianza presumida por el instrumento es tal en este caso que la autoridad competente de un Estado miembro hace la petición directamente al proveedor de servicios, sin requerir, en principio, la intervención de las autoridades de ese Estado. La orden europea de entrega o de conservación puede dar lugar, en su caso, a la intervención de una autoridad judicial del Estado de ejecución para hacer cumplir la decisión, pero no interviene para tramitarla por defecto¹⁰. En este sentido, es el Parlamento quien propuso que, en el caso de la entrega de datos de tráfico y contenido, la autoridad del Estado de ejecución fuera notificada con un efecto suspensivo que, inicialmente, el Consejo denegó¹¹.

Por lo tanto, es el representante legal de un actor privado, y no una autoridad, quien recibirá la orden judicial. Creemos que otorgar este rol a un actor privado, del que se presume que actúa en su propio beneficio y no por el interés general o la protección

7. Vid., por ejemplo, los asuntos TJUE, 24 de junio de 2019, *Comisión c. Polonia*, C-619/18; TJUE, 17 de julio de 2021, *Comisión c. Polonia*, C-791/19, entre muchos más.

8. Art. 7, apartado 1 y art. 7, apartado 2, de la propuesta.

9. Considerando (11); art. 9 y 10 de la propuesta.

10. Art. 14 de la propuesta.

11. Note from General Secretariat of the Council to Delegations, Interinstitutional files 2018/0107(COD) 2018/0108(COD), p.4.

de los derechos de los individuos, abre el camino a una nueva y mucho más profunda ola de objeciones en el ámbito de los datos personales, que ya han sido objeto de disputas constitucionales en los Estados miembros, quienes reclaman su competencia en materia de seguridad¹². De esta manera, además, en la propuesta de Reglamento estudiada, el reconocimiento mutuo es llevado hasta un grado de “automatismo” elevado, tanto a través de los limitados motivos de oposición previstos (de carácter técnico y no sustancial, como veremos más adelante), como por la misma naturaleza privada de quien tiene que ponerlos en práctica.

En las condiciones actuales, cabe muy bien esperar que el demandado, si tiene conocimiento del requerimiento en su contra¹³, desconfíe del representante legal del prestador de servicios (que él mismo designa), una empresa grande y distante que tomará una decisión que determinará en parte la suerte de sus derechos procesales y libertades fundamentales en materia penal. De hecho, se han previsto sanciones si no lo hace¹⁴. Esto conduce a una forma de privatización de la justicia y a una probable disminución de confianza en ella o, al menos, en su apariencia. Es además el mismo prestador quien debe informar, a la persona cuyos datos se solicitan, de la posibilidad de utilizar vías de recurso. Si el prestador de servicios no lo hace a petición de la autoridad emisora, esta informará a la persona cuando ya no haya riesgo de poner en peligro la investigación y le facilitará la información necesaria sobre los recursos legales. Dado que a la orden europea de conservación se le presupone una menor interferencia en los derechos afectados, la información solo será facilitada en el caso de las órdenes europeas de entrega¹⁵. Por lo tanto, una autoridad judicial intervendrá, eventualmente, *a posteriori*, una vez la entrega haya tenido lugar, y tan solo si el afectado impugna la legalidad de dicha entrega. Hoy por hoy no se prevén, pues, vías de recurso ante la “mera” conservación de los datos¹⁶.

Con todo, creemos que es dudoso que, en el caso de una eventual vulneración del Estado de Derecho en un país que emita una EPOC o EPOC-PR, estas disposiciones sean capaces de blindar al legislador ante un contencioso judicial como el que sigue existiendo en entorno a la ODE¹⁷. Hemos podido observar en estos casos que la limitación de los motivos de denegación para reclamar el reconocimiento casi-automático

12. Vid., en este sentido los asuntos *Privacy International C-623/17*; *La Quadrature du Net e.a. C-511/18* y *French Data Network e.a. C-512/18*, así como *Ordre des barreaux francophones et germanophone et a. C-520/18*.

13. El artículo 11 de la propuesta permite a los proveedores de servicios abstenerse de informar a la persona cuyos datos se solicitan si la autoridad emisora así lo pide, con el fin de proteger la confidencialidad de la investigación criminal.

14. Art. 13 de la propuesta.

15. Art. 11 de la propuesta.

16. Art. 17, apartado 1, de la propuesta.

17. Vid., entre otros, los asuntos *Aranyosi y Caldaru (C-404/15 y C-659/15 PPU)*; *Doroban-tu (C-128/18)*, *LM (C-216/18)* y *Romeo Castaño (n.º 8351/17)*. Los jueces luxemburgueses han respondido a estos casos con ajustes jurisdiccionales al principio de la confianza mutua, que también ha sido cuestionado en España (Vid., por un asunto reciente, *Puig Gordi y o. C-158/21*).

no ha evitado la batalla jurídica en un contexto que hace cada vez más inestable la confianza entre Estados¹⁸. Además, constataremos que, en el caso que nos ocupa, la ausencia de apreciación por parte del destinatario del requerimiento se da también atendiendo a dichos motivos de denegación. Tratándose formalmente de un actor privado, es lógico esperar que su poder de decisión resulte, en la práctica, menguado.

Más directamente, la obligación de cumplir con las órdenes es imperativa¹⁹. Creemos que este principio de obligatoriedad teórica se ve confirmado por las disposiciones que rigen el modo de funcionamiento práctico de este mecanismo, que lo destinan a una inmediatez sistemática.

2.2. Una evaluación parcialmente neutralizada

La mayoría de las eventualidades previstas que puedan imposibilitar el cumplimiento de la orden (que no se encuentran en una lista a modo de uso facultativo, sino que son presentadas como excepciones) tienen una naturaleza técnica. Así, se refieren a la validación, la imposibilidad material o la presentación de errores en la orden —en cuyo caso el destinatario advertirá a la autoridad emisora—. Solo una hipótesis de denegación presenta una naturaleza sustancial y confiere cierto margen de apreciación al requerido: la prueba de que el contenido de las órdenes infringe manifiestamente la Carta o es manifiestamente abusivo²⁰. El Consejo, en la posición que adoptó sobre el reglamento²¹, propuso suprimir esta disposición, mientras que el Parlamento insistió en añadirla como motivo de denegación de la ejecución²². Finalmente, en el texto transaccional final²³, la disposición se ha mantenido, con una

18. Para un análisis de la ya clásica tensión entre los mecanismos de reconocimiento mutuo y la crisis de los valores de la UE, vid. MARGUERY, Tony. *Confiance mutuelle, reconnaissance mutuelle et crise de valeurs, la difficile équation entre justice pénale européenne et diversité nationale*. *European papers: a journal on law and integration*. 2020, <https://dialnet.unirioja.es/ejemplar/590319>, vol. 5(3), pp. 1271-1288 [fecha de consulta: 01.07.2023]. Recuperado de: <https://www.europeanpapers.eu/en/e-journal/confiance-mutuelle-reconnaissance-mutuelle-crise-de-valeurs>.

19. Como se deduce de los términos de la redacción de los artículos 9 y 10 de la propuesta.

20. Art. 14. 4 (g) y 14. 5 (f) de la propuesta.

21. General approach- Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters, 7 December 2018, art. 14.2a (p.43).

22. Note from General Secretariat of the Council to Delegations, Interinstitutional files 2018/0107(COD) 2018/0108(COD), p.4.

23. Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. Interinstitutional File: 2018/0108(COD), Brussels, 20 January 2023, from Presidency to Permanent Representatives Committee.

redacción que ilustra claramente su vocación de excepcionalidad²⁴. Es también el Parlamento quien propuso derogar automáticamente la ejecución cuando la autoridad emisora proceda de un Estado contra el que se haya incoado el procedimiento del artículo 7 del Tratado de la Unión Europea²⁵, impulsando así, sin éxito, la creatividad en defensa del Estado de Derecho.

En cualquier caso, creemos que, en la práctica, no serán numerosos los casos de oposición por parte del prestador de servicios o de su representante, siendo que previamente una autoridad judicial del Estado emisor habrá verificado la validez de la orden²⁶. Es razonable prever entonces una cierta “intimidación legal” por parte del proveedor de servicios en el contexto de la cooperación entre autoridades que son de distinta naturaleza; no olvidemos que el proveedor no tiene por qué ser un conocedor de las prácticas jurídicas. Sin embargo, en el caso que ahora nos ocupa, para saber si debe oponerse a la ejecución del requerimiento, se le pide que identifique los privilegios e inmunidades de un sospechoso o acusado, o incluso que conozca las normas de un país tercero que prohibirían la revelación de datos en aras a la protección de derechos fundamentales o de intereses de seguridad y de defensa de ese país, y que determine si existe alguna contradicción con las órdenes recibidas²⁷.

La oposición por parte del proveedor se hace mucho menos probable teniendo en cuenta las modalidades de ejecución previstas, que reflejan la celeridad que caracteriza al mecanismo estudiado. El destinatario está obligado a responder en un plazo de 10 días, y de 8 horas en caso de urgencia (frente a los hasta 120 días de la orden europea de investigación o los 10 meses de un procedimiento de asistencia judicial)²⁸.

Pero no solo es objetable la configuración procedimental del mecanismo, sino que, al analizar la interferencia del contenido de la medida con los derechos fundamentales, surgen también cuestiones relacionadas con la solidez de las garantías, las cuales, creemos, se hacen todavía más exigibles en un escenario caracterizado por la volatilidad.

24. Las órdenes podrán no ser ejecutadas si [basándose únicamente en la información contenida en la EPOC/EPOC-PR, resulta evidente que, en situaciones excepcionales, existen motivos fundados para creer, sobre la base de pruebas concretas y objetivas, que la ejecución de la orden supondría, en las circunstancias particulares del caso, una violación manifiesta de un derecho fundamental *importante*, de conformidad con el artículo 6 del TUE y la Carta] -cursiva y traducción propias, del art. 14. 4 (g) y 14. 5 (f) del texto transaccional definitivo del 20 de enero de 2023 (Interinstitutional File: 2018/0108(COD)).

25. European Parliament Report, 11 December 2020, COM (2018)0225 – C8-0155/2018 – 2018/0108(COD), Point (11a).

26. Art. 4 de la propuesta.

27. Art. 16 de la propuesta.

28. Art. 9 de la propuesta; European Commission, Frequently Asked Questions: New EU rules to obtain electronic evidence https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345.

3. LA INJERENCIA EN LOS DERECHOS FUNDAMENTALES

Una vez analizada la configuración del mecanismo, planteamos en este punto, que la proporcionalidad de la injerencia en los derechos fundamentales parece dudosa (3.1), a la vez que su legitimidad resulta cuestionable (3.2).

3.1. *Una protección mermada de los datos personales*

En la propuesta de Reglamento relativo a las órdenes de entrega y conservación de pruebas electrónicas, se encuentra especialmente en juego el derecho a la protección de los datos personales.

Esta cuestión que aquí nos ocupa es tanto más delicada cuanto que las órdenes pueden abarcar cualquier categoría de datos. En efecto, la medida propuesta no solo abarca los metadatos de las comunicaciones, sino que también afecta a los “datos de contenido”. Estamos hablando, pues, de todos los datos almacenados en formato digital, como texto, voz, vídeo, imágenes y sonido. Es con esta lógica que se establece en la propuesta un régimen más estricto para los datos de contenido y de tráfico (excepto aquellos solicitados con el único fin de identificar al usuario), de modo que solo sea posible solicitar la entrega de los mismos por delitos con penas superiores a 3 años, excepción hecha del terrorismo, la ciberdelincuencia, la pornografía infantil y la falsificación de medios de pago distintos del efectivo²⁹. La exclusión de determinadas formas delictivas más leves es, por lo tanto, numérica y no nominativa (se hace por la sanción y no a raíz de la tipificación), lo que implica que no se haya previsto para este mecanismo ninguna regla de doble incriminación, excepto en el caso de intervención de la autoridad estatal³⁰.

La excepcionalidad que rodea a estos tipos de delitos graves se manifestaba igualmente en un segundo supuesto que fue añadido por el Consejo, si bien no ha sido reproducido en el texto de compromiso final: el principio de especialidad. Los miembros de la institución habían inicialmente establecido que los datos solicitados no podrían utilizarse para fines distintos de aquellos para los que se obtuvieran, excepto en los casos de prevención de una amenaza grave e inmediata para la seguridad pública o los intereses esenciales del Estado emisor o a efectos de un procedimiento para el que podría haberse dictado una orden de entrega³¹.

29. Art. 5, apartado 4, de la propuesta. Sobre esta excepción, vid. los problemas de proporcionalidad planteados por TINOCO-PASTRANA, Angel. The Proposal on Electronic Evidence in the European Union. *Eucrim* [en línea] Max Planck. 2020, Nº 1, pp.46-50, [fecha de consulta: 01.02.2023]. Disponible en: <https://doi.org/10.30709/eucrim-2020-004>.

30. Art. 10a, añadido en la reciente versión del 20 de enero de 2023 de la propuesta.

31. General approach- Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters, 7 December 2018, art. 12b (p.41).

Es imperativo recordar aquí que, en el contexto de una Unión que pretende hacer de la protección de los derechos fundamentales una seña de identidad, el Tribunal de Justicia se ha propuesto actuar positivamente para contribuir al desarrollo de una protección que conciba la *privacy* como una prioridad. Esto es coherente con el hecho de que la Carta fuera el primer instrumento internacional de derechos humanos que recogió con carácter vinculante el derecho al respeto de los datos personales³². Digital Rights Ireland³³ es el ejemplo paradigmático de esta concepción garantista.

Remarquemos, no obstante, que en esta última decisión el juez invalidó la Directiva 2006/24, a la vez que precisó que la medida en cuestión, aun siendo desproporcionada, había dejado intacto el contenido esencial, ya que la conservación era de los metadatos y no de los contenidos de las comunicaciones. De una forma tradicionalmente oscura en la materia³⁴, el Tribunal pareció inferir que el contenido esencial e intangible correspondía al conocimiento del contenido de las comunicaciones. Sin embargo, de ser así, sería razonable considerar entonces que, en los términos en que está planteado hoy en día el Reglamento sobre la prueba electrónica, se afectaría al contenido esencial del derecho a la protección de datos de carácter personal³⁵.

3.2. Una intromisión progresivamente normalizada

Siguiendo con la lógica de la categorización, para la entrega de datos se ha previsto un régimen más estricto que para su conservación, y esta última puede hacerse no solo para los datos de abonados y relativos a la identificación del usuario³⁶, sino también para los de tráfico y contenido. La diferenciación de protección entre el régimen da a entender implícitamente que la conservación “no es tan intrusiva”. Es con esta misma lógica que a la persona cuyos datos son solicitados no le es posible recurrir una orden de conservación, que, además, puede ser emitida por un fiscal³⁷. Todo ello en el marco de un procedimiento que, como hemos visto, puede pasar por el cauce privado y totalmente desapercibido a la autoridad del Estado de ejecución.

32. Art. 8 de la Carta de Derechos Fundamentales.

33. TJUE, 8 abril 2014, *Digital Rights Ireland*, C-293/12 y C-594/12.

34. Vid., en este sentido, SCARCELLO, Orlando. Preserving the ‘Essence’ of Fundamental Rights under Article 52(1) of the Charter: A Sisyphean Task. *European Constitutional Law Review*. 2020, 16(4), p. 648, [fecha de consulta: 01.02.2023]. Disponible en: <https://doi.org/10.1017/S1574019620000395>.

35. Contenido que tiene que respetar toda limitación de derechos, según reza el art. 52, apartado 1, de la Carta de los Derechos Fundamentales de la UE.

36. Nótese que en el texto transaccional definitivo se ha cambiado la expresión “datos de acceso”, que figuraba en la propuesta inicial, por “datos solicitados con el único fin de identificar al usuario”.

37. Art. 4 de la propuesta. Queda por ver si el concepto aquí utilizado como “autoridad judicial” será suficientemente independiente para el Tribunal Europeo de Derechos Humanos, que tradicionalmente ha demostrado tener una concepción más exigente de esta noción (TEDH, 29 marzo 2010, *Medvedyev y otros c. France*, n.º 3394/03).

Sin embargo, en la ya citada sentencia *Digital Rights Ireland* y, más recientemente, en la decisión del mismo Tribunal de 5 de abril de 2022³⁸, la retención de datos de tráfico y localización fue considerada intrusiva. Igualmente, en la decisión del pasado 7 de septiembre el Tribunal de Luxemburgo recordaba que, de conformidad con el principio de proporcionalidad, solo la lucha contra la delincuencia grave y la prevención de amenazas graves para la seguridad pública pueden justificar una injerencia grave en los derechos fundamentales, como la que supone la *conservación de los datos de tráfico y de localización*³⁹. Las nuevas órdenes en materia de datos, a pesar de que tratan diferenciadamente sus categorías —buscando anticiparse a un nuevo reproche de desproporcionalidad por una retención generalizada—, hacen temer una normalización gradual hacia una injerencia en los mismos. Además, no podemos pasar por alto que el peligro de vulneración de los derechos fundamentales es tanto mayor por su componente inmaterial, el cual dificulta en gran manera el control de dicha injerencia.

Teniendo en cuenta la dirección de su jurisprudencia reciente, quedará por ver, si se aprueba el texto, si en el eventual caso de un recurso de anulación, el Tribunal validará el dispositivo del legislador, teniendo en cuenta la dirección de su jurisprudencia reciente.

El estándar de protección de datos personales que el legislador promoverá en su texto y la interpretación que el juez le dará serán tanto más cruciales cuanto que se propagarán a través de las relaciones con otros países, principalmente, Estados Unidos, donde se encuentran la mayoría de los proveedores de servicios electrónicos.

En efecto, las disposiciones *e-evidence* afectan a los proveedores de servicios que “ofrecen servicios en la Unión”⁴⁰. Esta amplia inclusión, combinada con la intangibilidad de los datos y su componente transnacional, facilita la difusión de la legislación de la UE más allá de sus fronteras. Tras la invalidación del *Privacy Shield* por la justicia europea⁴¹, las autoridades deberán aplicar en breve un acuerdo que regule las transferencias transatlánticas de datos. Creemos que es necesario que la UE se afirme y no haga concesiones en materia de privacidad electrónica y derechos procesales del ciudadano digital. Ciertamente, en el campo de la protección de datos, el “Brussels Effect”⁴² encuentra su máxima expresión.

38. TJUE, 5 de abril de 2022, *Commissioner of the Garda Síochána e.a.*, C-140/20.

39. TJUE, 7 de septiembre de 2023, *Lietuvos Respublikos generalinė prokuratūra*, C-162/22. Las cursivas de la frase han sido añadidas por nosotros. Las nuevas órdenes en materia de datos, a pesar de que tratan diferenciadamente sus categorías —buscando anticiparse a un nuevo reproche de desproporcionalidad por una retención generalizada—, hacen temer una normalización gradual hacia una injerencia en los mismos. Además, no podemos pasar por alto que el peligro de vulneración de los derechos fundamentales es tanto mayor por su componente inmaterial, el cual dificulta en gran manera el control de dicha injerencia.

40. Art. 2.4 (b) y art. 3.1 de la propuesta.

41. TJUE, 16 de julio de 2020, «*Schrems II*», C-311/18.

42. En la expresión de Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. London: Oxford University Press, 2020.

4. CONCLUSIONES

En este trabajo nos hemos propuesto llevar a cabo un breve análisis de la configuración formal y material de la propuesta de Reglamento sobre pruebas electrónicas, a través de los actos de las instituciones europeas involucradas en él. Si bien es cierto que el texto transaccional final es más protector que la propuesta inicial, especialmente, por erigir la infracción de un derecho fundamental en un supuesto de denegación de la ejecución o por la notificación a la autoridad del Estado de ejecución prevista en algunos casos, siguen existiendo, a nuestro parecer, importantes lagunas en lo que respecta a la protección de derechos fundamentales, tanto en su vertiente procesal como sustancial.

En el primer caso, hemos visto que, de las razones para oponerse a la ejecución de una orden de entrega o de conservación, se desprende el carácter operativo de este tipo de mecanismo. La naturaleza no jurisdiccional del proveedor de servicios electrónicos y los motivos formales de oposición, combinados con el pretexto de la urgencia, sugieren que los supuestos en los que el proveedor se opondrá al requerimiento serán muy limitados. Es por todo ello que hemos considerado que se trata de un dispositivo que tiende sobre todo a la eficacia de las investigaciones.

En el segundo, y como consecuencia de esto último, la protección de los datos personales nos parece defectuosa, sobre todo en lo que respecta a los datos de contenido. Si bien creemos que la categorización busca respetar formalmente el principio de proporcionalidad, el alcance real del dispositivo dependerá de la posición mantenida por el Tribunal de Justicia de la Unión Europea (TJUE), dado el caso. Sin embargo, en el estado actual del derecho de la UE, nos parece como mínimo preocupante que esta propuesta legitime la injerencia en los datos personales, manteniendo un estándar menos garantista y más intrusivo, cuando el grado o la finalidad de esta no se expresa en su máxima intensidad, es decir, cuando se trata de datos de abonados y relativos a la identificación del usuario, o cuando los datos se solicitan “solamente” a efectos de conservación.

Con todo, su eficacia en términos de recepción y comunicación de pruebas parece evidente.

No estamos en medida de decir si el fin justifica los medios. Sin embargo, sí sabemos que el nuevo Reglamento propuesto por la Comisión no sustituirá la Directiva relativa a la orden europea de investigación en lo que respecta a la obtención de pruebas electrónicas, sino que proporcionará una herramienta adicional a las autoridades.

Quedará por evaluar, pues, el valor añadido concreto de las órdenes europeas de conservación y entrega de datos, cuya aplicación se antoja complicada, como mínimo, debido a la naturaleza técnica de las pruebas electrónicas⁴³. Sin embargo,

43. Se han planteado ya dificultades en relación con la orden europea de investigación. Han sido identificadas tanto en la fase de emisión, por su formalismo, como en la fase de ejecución, en particular por la insuficiente armonización de las legislaciones nacionales (Informe de la Comisión al Parlamento y al Consejo, de 20 de julio de 2021, sobre la aplicación de la Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal).

como el reglamento propuesto prevé plazos más breves que los previstos en la orden europea de investigación, podemos suponer que, en materia penal, las nuevas EPOC y EPOC-PR serán el instrumento preferido por las autoridades que recogen pruebas electrónicas. La excepcionalidad que a la luz de un régimen que interfiere en libertades fundamentales debería caracterizarla corre el riesgo de tornarse, en la práctica, más bien hipotética.

Todo ello se sitúa en los fundamentos de los mecanismos de cooperación judicial, de los que hemos partido, en cuyo seno se ha venido exigiendo tradicionalmente el reconocimiento mutuo entre autoridades de Estados miembros. Hemos visto que en el caso de la prueba electrónica dicho reconocimiento se ha confiado a una empresa, a un actor privado. Parece que asistimos, pues, más que a una sublimación de la confianza mutua, a una forma de privatización de la misma, a la vez que se confiere al proveedor de servicios una práctica casi-judicial.

Por añadidura, la era de la digitalización va acompañada de una intangibilidad que la hace aún más difícil de aprehender. Un nuevo reto ha surgido en este contexto: comprender una nueva realidad criminológica. Para ello, disponemos de conceptos tradicionales, los cuales requieren una revisión y adaptación o la creación de otros nuevos que conceptualicen adecuadamente el ciberespacio, especialmente en el seno del particular ordenamiento jurídico de la UE.

Al mismo tiempo, y yendo más allá de la cooperación procedimental, es necesaria una solidificación de los principios generales que deben orientar la armonización sustancial de conductas delictivas. Una mayor claridad y coherencia con los principios fundamentales del derecho penal, aparejada con una innegable incrementada eficacia a escala europea en la lucha contra las formas transnacionales de delincuencia, consolidaría la legitimidad de la UE a la hora de sancionar. Esperemos que también se afiancen progresivamente sus competencias generales en materia penal, ya sea, al menos, en aras a una mayor eficacia procesal.

De lo contrario, si no actuamos en una fase preventiva, será una crisis de seguridad cibernética sistémica la que nos empujará a dar pasos de gigante, movidos por la necesidad de la emergencia, y viéndonos obligados a abandonar, ante la urgencia, las deseadas garantías. Y en ese escenario, todo resultará aún menos evidente.

5. REFERENCIAS

- AMBOS, Kai, 2021. 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 Llorente Sánchez-Arjona, Mercedes (Dir.). *Estudios procesales sobre el espacio europeo de justicia penal*. Cizur Menor: Aranzadi, 2021, pp. 141-169.
- BRADFORD, Anu, 2020. *The Brussels Effect: How the European Union Rules the World*. London: Oxford University Press. <https://doi.org/10.1093/oso/9780190088583.001.0001>

- COMISIÓN EUROPEA, 2021. *Informe de la Comisión al Parlamento y al Consejo, de 20 de julio de 2021, sobre la aplicación de la Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal*. Recuperado de <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021DC0409&from=ES>
- CONSEJO DE LA UNIÓN, 2002. *Decisión Marco del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (2002/584/JAI)*. Diario Oficial n° L 190 de 18/07/2002 p. 0001 - 0020. Recuperado de: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32002F0584>
- COUNCIL, 2018. *Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters. (General approach, 7 December 2018)*. Recuperado de: <https://data.consilium.europa.eu/doc/document/ST-15292-2018-INIT/en/pdf>
- COUNCIL, 2022. *Note from General Secretariat of the Council to Delegations, Interinstitutional Files 2018/0107(COD), 2018/0108(COD). Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. Brussels, 16 June 2022*. Recuperado de: <https://www.statewatch.org/media/3390/eu-council-e-evidence-presidency-note-10271-22.pdf>
- COUNCIL, 2023. *Note from Presidency to Permanent Representatives Committee, Interinstitutional File: 2018/0108(COD). Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, Brussels, 20 January 2023*. Recuperado de: <https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf>
- EUROPEAN COMMISSION, 2018. *Frequently Asked Questions: New EU rules to obtain electronic evidence. 17 April 2018*. Recuperado de: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
- MARGUERY, Tony, 2020. *Confiance mutuelle, reconnaissance mutuelle et crise de valeurs: la difficile équation entre justice pénale européenne et diversité nationale. European papers: a journal on law and integration*, <https://dialnet.unirioja.es/ejemplar/590319>, Vol. 5 (3), 2020, pp. 1271-1288 [fecha de consulta: 01.07.2023]. Recuperado de: <https://www.europeanpapers.eu/en/e-journal/confiance-mutuelle-reconnaissance-mutuelle-crise-de-valeurs>
- PARLAMENTO EUROPEO, 2020. *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. (COM(2018)0225 – C8-0155/2018 – 2018/0108(COD))*. Recuperado de: https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_ES.html
- PARLAMENTO EUROPEO Y CONSEJO, 2014. *Directiva 2014/41/CE del Parlamento Europeo y del Consejo de 3 de abril de 2014 relativa a la orden europea de investigación en materia penal. Diario Oficial de la Unión Europea, 03/04/2014*. Recuperado de: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014L0041>
- PARLAMENTO EUROPEO Y CONSEJO, 2023. *Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo de 12 de julio de 2023 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*. Recuperado de: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32023L1544>

- SCARCELLO, Orlando, 2021. Preserving the 'Essence' of Fundamental Rights under Article 52(1) of the Charter: A Sisyphean Task. *European Constitutional Law Review*. 2020, 16(4), pp. 647-668, [fecha de consulta: 01.02.2023]. Disponible en: <https://doi.org/10.1017/S1574019620000395>
- TINOCO-PASTRANA, Angel, 2020. The Proposal on Electronic Evidence in the European Union. *Eucrim* [en línea], Max Planck. 2020, Nº 1, pp.46-50. [fecha de consulta: 01.02.2023]. Disponible en: <https://doi.org/10.30709/eucrim-2020-004>