INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 15 VOL. 1, 2024, PP. 33-46

EL REGLAMENTO EUROPEO *E-EVIDENCE* Y EL BALANCE ENTRE LA PROTECCIÓN DE DATOS Y LA SEGURIDAD TRANSFRONTERIZA

THE EUROPEAN REGULATION ON E-EVIDENCE AND THE BALANCE BETWEEN DATA PROTECTION AND CROSS-BORDER SECURITY

Sarah Rachut
Julian W. Maurer
TUM Center for Digital Public Services, Technical University of Munich (Alemania)

Resumen

El presente artículo examina el Reglamento *E-Evidence*, adoptado por la Unión Europea en junio de 2023, el cual establece un marco legal para la cooperación transfronteriza en la obtención de pruebas electrónicas en investigaciones penales. Este reglamento surge de la necesidad de facilitar la obtención de pruebas almacenadas en el extranjero, especialmente en investigaciones relacionadas con terrorismo, fraude y delitos sexuales contra menores. El artículo revisa los antecedentes que llevaron a la creación del reglamento y muestra al lector una introducción en los dos instrumentos principales del nuevo Reglamento sobre la prueba electrónica: la Orden Europea de Producción y la Orden Europea de Conservación, permitiendo a las autoridades judiciales solicitar y preservar datos electrónicos de proveedores de servicios en otros Estados miembros de la UE.

Además, el artículo compara el Reglamento sobre la prueba electrónica con el *CLOUD Act* de Estados Unidos, destacando similitudes y diferencias, y analiza críticas, especialmente en cuanto a la protección de datos y la posible erosión de los derechos individuales. Se discute el impacto potencial del reglamento y la necesidad de seguimiento y evaluación continuos para prevenir abusos y garantizar el respeto a los principios del Estado de Derecho.

Palabras clave

Prueba electrónica, regulación en la nube, protección de datos, delitos informáticos, tecnología.

Abstract

This article examines the *E-Evidence* Regulation, adopted by the European Union in June 2023, which establishes a legal framework for cross-border cooperation in obtaining electronic evidence in criminal investigations. This regulation arises from the need to facilitate the collection of evidence stored abroad, especially in investigations related to terrorism, fraud, and sexual offences against children. The article reviews the background that led to the creation of the regulation and introduces the reader to the two main instruments of the new *E-Evidence* Regulation: the European Production Order and the European Preservation Order, allowing judicial authorities to request and preserve electronic data from service providers in other EU Member States.

In addition, the article compares the *E-Evidence* Regulation with the US CLOUD Act, highlighting similarities and differences, and analyses critics, especially in terms of data privacy issues and the potential erosion of individual rights. It also discusses the potential impact of the regulation and the need for continuous monitoring and evaluation to prevent abuses and ensure respect for rule of law principles.

Keywords

E-Evidence, CLOUD Act, data protection, cybercrime, technology.

Introducción

Las pruebas electrónicas tienen especial importancia en casi el 85 % de las investigaciones penales dentro de la Unión Europea, pero el 65 % de ellas suele obtenerse originariamente de otros países europeos distintos del Estado miembro investigador (Parlamento Europeo, 2023).

Especialmente en el contexto de las investigaciones antiterroristas, pero también en la persecución de fraude y de delitos sexuales contra menores. Asimismo, los investigadores de los Estados miembros precisan pruebas suficientemente completas y fiables. Sin embargo, a menudo estas pruebas se encuentran en el espacio digital y, por tanto, fuera del control de las autoridades policiales de los Estados miembros particulares, como España o Alemania. Con el *Reglamento sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales (Reglamento E-Evidence* o *Reglamento sobre la prueba electrónica)* (Unión Europea, 2023b), la Unión Europea creó un marco jurídico para facilitar la cooperación transfronteriza entre las autoridades encargadas de la investigación penal y los proveedores de servicios que operan dentro de la Unión Europea, independientemente de si almacenan los datos de posibles sospechosos, sus usuarios, en servidores dentro o fuera de la Unión Europea.

El presente artículo esbozará principalmente los antecedentes y la historia del desarrollo del Reglamento sobre la prueba electrónica antes de pasar a explicar con más detalle los aspectos específicos del contenido normativo y los instrumentos concretos. A continuación se discutirá el Reglamento en el contexto del *Clarifying Lawful Overseas Use of Data Act* (*CLOUD Act*) de los EE. UU. y se expondrán sus similitudes y diferencias antes de formular una serie de críticas.

Antecedentes y trayectoria del Reglamento *E-Evidence*

Debido al surgimiento del terrorismo islamista en el plano internacional, en el que se lleva viviendo desde hace ya más de una década, los ministros de justicia de la Unión Europea acordaron ya en marzo de 2016 dar prioridad a la creación de medidas para la obtención y la seguridad eficientes y eficaces de las pruebas electrónicas en el futuro. Estas deliberaciones vinieron precedidas, entre otros, por los atentados terroristas de París del 13 de noviembre de 2015, y los atentados terroristas de Niza del 14 de julio de 2016, de Berlín del 19 de diciembre de 2016 y, finalmente, de Barcelona del 17 de agosto de 2017 hicieron que el tema cobrara aún más relevancia (López Werner, 2023; Pacelli, 2023; Andreeva, 2020). En los atentados mencionados, los autores se habían comunicado en una medida nada desdeñable a través de canales de comunicación en línea en el período previo al delito y durante el mismo.

En un dictamen emitido por el Consejo de Justicia y Asuntos de Interior de la Unión Europea el 9 de junio de 2016, el Consejo concluyó, entre otras constataciones, que debe negarse a toda costa a los actores delictivos un «refugio seguro» en el ciberespacio y que será necesario actuar ante el creciente impacto de la

ciberdelincuencia como tal, pero también debido a las actividades delictivas que posibilita internet en general (Consejo de la Unión Europea, 2016). En concreto, el Consejo destacó la importancia de las pruebas electrónicas en los procesos penales, razón por la cual las autoridades policiales y judiciales de los Estados miembros deben estar dotadas de herramientas completas y eficaces para investigar y perseguir los delitos relacionados con el ciberespacio. En particular, el Consejo sugirió que se ampliara la cooperación entre los proveedores y las autoridades de seguridad. Con ello se agilizarán los procedimientos de asistencia judicial y se revisará la normativa relativa a la aplicación de la ley en el ciberespacio. Entre diciembre de 2016 y junio de 2017, los servicios de la Comisión publicaron otros documentos de trabajo, y este último documento, publicado el 8 de junio de 2017, también contenía propuestas de medidas sobre cómo mejorar específicamente el acceso a los documentos digitales y a la información en las investigaciones penales transfronterizas (Comission Services, 2017; Burchard, 2018).

Finalmente, las propuestas desarrolladas por la Comisión dieron lugar en 2018 al proyecto de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal (Reglamento *E-Evidence*), que la Comisión Europea presentó el 18 de abril de 2018. El Parlamento Europeo aprobó finalmente la propuesta ligeramente modificada el 13 de junio de 2023. Además del Reglamento sobre la prueba electrónica, se adoptó el 12 de julio de 2023, como parte del paquete *E-Evidence*, la llamada Directiva de Representantes (Unión Europea, 2023a), que regula la designación de sucursales y el nombramiento de representantes de determinados proveedores de servicios. Para facilitar la aplicación del Reglamento sobre la prueba electrónica, estos proveedores de servicios deberán designar representantes o establecimientos dentro de la Unión Europea encargados de recibir, cumplir y hacer cumplir las decisiones y órdenes emitidas por las autoridades de investigación.

Disposiciones e instrumentos del Reglamento *E-Evidence*

El núcleo del Reglamento sobre la prueba electrónica adoptado es la introducción de los instrumentos de una *Orden Europea de Producción* y una *Orden Europea de Conservación*, en virtud de los cuales estas deben ser expedidas o validadas por la autoridad judicial competente de un Estado miembro en su aplicación específica según la propuesta. El art. 3 n.º 1 del Reglamento *E-Evidence* define la *Orden Europea de Producción* como

> una decisión por la que se ordena la entrega de pruebas electrónicas, emitida o validada por una autoridad judicial de un Estado miembro (…), y dirigida a un establecimiento designado o a un representante legal de un prestador de servicios que ofrezca servicios en la Unión, cuando dicho establecimiento designado o representante legal esté situado en otro Estado miembro (…).

La *Orden Europea de Conservación*, por su parte, se define como

> una decisión por la que se ordena la conservación de pruebas electrónicas a los efectos de una solicitud posterior de entrega, y que es emitida o validada por una autoridad judicial de un Estado miembro (…), y dirigida a un establecimiento designado o a un representante legal de un prestador de servicios que ofrezca servicios en la Unión, cuando dicho establecimiento designado o representante legal esté situado en otro Estado miembro (…). (Art. 3, num. 2 del Reglamento *E-Evidence*).

Estas órdenes deben aplicarse en particular cuando los datos hayan sido almacenados por un proveedor de servicios de otro país, y puedan a su vez ser relevantes como prueba en el contexto de investigaciones o procesos penales. De conformidad con el art. 3, num. 3 del Reglamento *E-Evidence*, los proveedores de servicios son aquellas personas físicas o jurídicas que ofrecen uno de los servicios definidos con en el art. 3, num. 2, lits. *a* a *c* (incluidos servicios de comunicaciones electrónicas, servicios de nombre de dominio de internet y de direcciones IP, tales como asignación de direcciones IP, registro de nombres de dominio, registrador de nombres de dominio y servicios de privacidad y representación relacionados con nombres de dominio y otros servicios de la sociedad de la información). En este contexto, debe tenerse en cuenta que la ejecución de una Orden Europea de Producción o de Conservación solo será admisible en la proporción en que sería posible adoptar una medida similar en una situación hipotética comparable en el territorio nacional del Estado de emisión. En este contexto, cabe señalar también que el Reglamento sobre la prueba electrónica no contempla ninguna medida específica de vigilancia, ni siquiera incluye normas sobre la retención de metadatos. El objetivo del reglamento se centra más bien en la facilitación de la labor de la autoridad de instrucción penal en la fase de investigación y enjuiciamiento en cada caso concreto, por lo que el ámbito de aplicación de los instrumentos previstos se extiende exclusivamente a las fases que abarcan desde la investigación previa al juicio hasta la respectiva resolución del procedimiento por archivo o sentencia. La entrega de datos de abonado y de acceso puede solicitarse en todas las diligencias penales, mientras que la entrega de datos de transacción y de contenido solo se permite cuando se trata de delitos punibles en el Estado de emisión con una pena privativa de libertad mínima de tres años (véase el artículo 5.3 y 5.4 lit. *a* del Reglamento *E-Evidence*).

Las excepciones son los actos delictivos ya señalados explícitamente en la propuesta legislativa, cuando pueda establecerse un vínculo suficiente entre el uso de los sistemas de información y el hecho delictivo en cuestión (en particular en materia de lucha contra el fraude y la falsificación en relación con los medios de pago distintos del efectivo, los abusos sexuales y la explotación sexual de menores y la pornografía infantil, así como los ataques contra los sistemas informáticos; véase el artículo 5.4, lit. *b*, del Reglamento *E-Evidence*) o los delitos que entran en el ámbito de aplicación de la Directiva de la Unión Europea (2017) relativa a la lucha contra el terrorismo (artículo 5.4, lit. *c*, del Reglamento *E-Evidence*).

En cuanto a la ejecución de una Orden Europea de Producción, el Reglamento *E-Evidence* establece que los datos solicitados deben transmitirse a la autoridad de emisión o a la autoridad fiscal competente en un plazo máximo

de diez días a partir de la recepción de la orden, aunque en casos excepcionales podría ser conveniente tramitarlos antes (art. 9.1 del Reglamento *E-Evidence*). En casos de emergencia, los datos solicitados deben tramitarlos incluso inmediatamente, pero a más tardar en un plazo de seis horas a partir de la recepción de la orden (art. 9.2 del Reglamento *E-Evidence*). En el caso de las órdenes de mera conservación, los datos solicitados deben conservarse inmediatamente de conformidad con el artículo 10.1, del Reglamento *E-Evidence*, según el cual esta conservación finaliza a los sesenta días, a menos que la autoridad emisora confirme al proveedor de servicios que se ha iniciado una solicitud de entrega. En tal caso, el proveedor de servicios deberá conservar los datos durante el tiempo necesario para entregarlos tras la recepción de la solicitud de entrega (art. 10.2 del Reglamento *E-Evidence*). Por lo tanto, en el sistema de órdenes, la Orden Europea de Conservación sólo sirve para preservar datos para ocasiones específicas, cuya entrega podría ordenarse posteriormente en el curso ulterior del procedimiento. Tras la solicitud de una autoridad, existen por lo general tres escenarios posibles: En el mejor de los casos, el proveedor de servicios coopera y transmite los datos a la autoridad de ejecución, que a su vez los transmite a la autoridad solicitante (Magno, 2023, p. 26). Si el proveedor de servicios rechaza la solicitud, los motivos deben ser evaluados por la autoridad de ejecución, que entonces ejecuta la orden o pide más información a la autoridad de origen. En caso de que la autoridad de ejecución llegara a la conclusión de que la orden no puede ejecutarse, deberá ponerse en contacto con la autoridad de origen (Magno, 2023, p. 26).

Los procedimientos de investigación criminal y la protección de datos

Incluso antes de la entrada en vigor del Reglamento *E-Evidence*, las cuestiones de seguridad y protección de datos no eran en absoluto irrelevantes en el contexto de los procedimientos de obtención de pruebas. De hecho, en el marco de las investigaciones policiales y fiscales también se procesan regularmente datos personales. En general, los datos personales están sujetos a la protección especial del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (Reglamento general de protección de datos, RGPD) (Unión Europea, 2016). En definitiva, el RGPD entiende como datos personales cualquier información sobre una persona física identificada o identificable. Asimismo, se considera como persona física identificable

> toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. (Art. 4.1 RGPD).

Con respecto al tratamiento de datos personales, se entiende como tal

> cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. (Art. 4.2 RGPD).

Sin embargo, debe tenerse en cuenta que la aplicabilidad del RGPD a los datos personales obtenidos durante las investigaciones penales debe excluirse de manera coherente. Esto también se desprende claramente del mismo Considerando n.º 19 del RGPD, que señala que las disposiciones del RGPD no son aplicables a las investigaciones penales. De lo contrario, sería inconcebible una labor de investigación significativa y eficaz. La protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales, incluidas la protección y la prevención de amenazas para la seguridad pública, y la libre circulación de dichos datos se regulan, por tanto, en un instrumento independiente de la legislación europea (Considerando n.º 19, apartado 1, frase 1). Por lo tanto, el RGPD no se aplicará explícitamente a las actividades de tratamiento con fines de investigación (Considerando n.º 19, apartado 1, frase 2).

Sin embargo, debido a la creciente relevancia de conductas delictivas cibernéticas vistas en los últimos años, el solapamiento entre las actividades de investigación de las autoridades y la participación de entidades privadas en los procedimientos de investigación es cada vez mayor. En una época en la que gran parte de la vida de los ciudadanos de la Unión Europea transcurre en el espacio digital y en la que las posibilidades de conservación de datos (sin autorización previa) están justamente restringidas, resulta cada vez más difícil distinguir entre la gestión de datos de carácter puramente oficial y la de carácter privado. Ello también se manifiesta en la práctica en las cadenas de cooperación de intervinientes privados, por ejemplo las grandes empresas tecnológicas, por un lado, y los investigadores públicos, por otro (Robinson, 2023, p. 2). No obstante, diversas formas y niveles de tratamiento de datos se ven afectados por esta circunstancia.

El Reglamento *E-Evidence* en el contexto de las iniciativas transatlánticas

Se puede contemplar la *CLOUD Act* estadounidense como el homólogo transatlántico del Reglamento sobre la prueba electrónica (US Department of Justice, 2018; Abraha, 2020, pp. 324-325).

Así pues, con el *CLOUD Act* a un lado del Atlántico y el Reglamento *E-Evidence* al otro, se enfrentarán dos actos jurídicos con una orientación similar, pero marcos jurídicos diferentes.

De hecho, el planteamiento de la Unión Europea va algo más lejos que el homólogo estadounidense del Reglamento sobre la evidencia electrónica. Mientras

que el *CLOUD Act* únicamente estipula que los proveedores de servicios estadounidenses están obligados a revelar los datos almacenados en caso de solicitud de revelación por parte de las autoridades de los EE. UU., incluso si se encuentran en un servidor fuera del país, el Reglamento *E-Evidence* establece que los proveedores de servicios deben revelar siempre los datos en cuestión, sin diferenciar dónde y quién los almacena. Esta obligación de información se aplica íntegramente a todos los proveedores de servicios que operan en la Unión Europea, independientemente de que sean o no empresas originariamente europeas. Por tanto, la obligación de revelar datos a las autoridades de los Estados miembros europeos también afectará a las empresas estadounidenses que no almacenen sus datos en Europa y les planteará nuevos retos en materia de protección de datos. En este sentido, para ellos, el potencial de conflicto en el marco de la legislación estadounidense de protección de datos surge del hecho de que, por regla general, las empresas estadounidenses no están autorizadas a entregar a las autoridades policiales de otros países datos sobre contenidos almacenados en EE. UU[1]. En consecuencia, las empresas estadounidenses se verán obligadas a incurrir en conductas prohibidas por la normativa de su país de origen. Este problema de protección de datos, que limitaría considerablemente la eficacia del Reglamento *E-Evidence* debido a su gran importancia, sólo podrá resolverse en última instancia mediante acuerdos correspondientes entre la UE y EE. UU. Sin embargo, es de suponer que una flexibilización de las correspondientes disposiciones de protección de datos de EE. UU. posiblemente se traduciría en un alto coste para el mismo, en términos de protección de datos por parte de la UE.

Crítica

Cuando se publicó por primera vez la versión del proyecto en 2018, la Comisión Europea ya se vio sometida a un amplio abanico de críticas, que desde entonces ya se habían suavizado. Sin embargo, a más tardar desde que se alcanzó el acuerdo político entre el Consejo Europeo y el Parlamento en enero de 2023, que en última instancia condujo a la adopción del Reglamento *E-Evidence* en el Parlamento Europeo el 13 de junio de 2023, el asunto ha vuelto a estar de actualidad.

El nuevo reglamento ha sido criticado, en particular, por cuestiones relacionadas con la protección de datos. Sin embargo, algunas otras disposiciones también son cuestionables a la luz del deterioro de la calidad del Estado de Derecho en algunos Estados miembros. Esto se aplica en particular al acceso a los datos de tráfico de internet, que pueden permitir sacar conclusiones precisas sobre la vida (privada) de una persona —siendo este último un peligro especialmente importante[2]—. A la vista de las enseñanzas extraídas del escándalo de las escuchas telefónicas *Pegasus*, en el que se reveló que Hungría, Polonia, España y Grecia, entre otros países, espiaban a ciudadanos políticamente indeseables (Raebisch, 2024, p. 65), puede criticarse sin duda una posibilidad exageradamente sencilla de acceso transnacional a datos sensibles.

1 *Vid*. también: Meissner (2023).

2 *Vid*. en este contexto también: Oromí i Vall-Llovera (2020).

Un cambio significativo, que también se debe en gran medida al debate crítico del primer borrador de la Comisión de 2018, se puede ver en el establecimiento del requisito de notificación del art. 13.1 del Reglamento *E-Evidence*, según el cual el interesado sobre el que se han solicitado los datos debe ser informado inmediatamente (De Hoyos Sancho, 2020, p. 108; Muriel Diéguez, 2024, p. 190). Únicamente se contemplan excepciones en los casos en que la notificación no parezca adecuada por razones de salvaguardia de las investigaciones o de protección de la seguridad nacional (art. 13.2 del Reglamento sobre la prueba electrónica).

Desde el punto de vista de la política jurídica, también resulta cuestionable hasta qué punto el Reglamento *E-Evidence* puede tener un efecto de modelo negativo. Con razón se apunta que el Reglamento podría servir de «modelo» para que los Estados no pertenecientes a la UE introduzcan normativas similares y que los Estados miembros de la UE podrían verse confrontados con órdenes de entrega que contribuirían a la persecución de delitos muy alejados de nuestras tradiciones jurídicas.

En este contexto, también hay que hacer especial referencia a las preocupaciones de la Conferencia Alemana de Protección de Datos, aún en relación con la actualmente suspendida legislación sobre conservación de metadatos en Alemania, que ya se expresaron en la fase de proyecto[3]. Estas son sumamente comprensibles, sobre todo teniendo en cuenta el pasado de Alemania y la fuerte brújula moral resultante, que hoy en día se refleja sobre todo en la defensa de los derechos humanos en todo el mundo. En particular, debido al deterioro de la calidad del Estado de Derecho en España (Hay Derecho, 2023) y algunos países de la Unión Europea (Gora y De Wilde, 2020), así como los recientes acontecimientos en España (por ejemplo, las circunstancias democráticamente cuestionables de la amnistía para los delincuentes separatistas catalanes (Ruíz Bursón, 2023, pp. 83, 122) o la falta de independencia política de la fiscalía y las autoridades de investigación españolas (Martínez Santos, 2022; Villoria Mendieta, 2022)), es preciso seguir de cerca la evolución y la aplicación del Reglamento *E-Evidence*. Especialmente porque, sobre todo en España, los supuestos delitos de responsables políticos o sus familiares a menudo se ven utilizados deliberadamente por corrientes políticas opuestas para debilitar a la oposición.

3 *Vid*.: «Besonders kritisch ist jedoch, dass in Deutschland Telekommunikationsdienstleister verpflichtet sind, u.a. sämtliche Verkehrsdaten für zehn Wochen zu speichern. Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen. Die Problematik dieser sog. Vorratsdatenspeicherung verschärft sich deutlich, wenn ausländische Strafverfolgungsbehörden einen direkten Zugriff auf derartige Informationen erhalten» («Sin embargo, resulta especialmente importante que los proveedores de servicios de telecomunicaciones en Alemania estén obligados, entre otras cosas, a almacenar todos los datos de tráfico durante diez semanas. Estos datos pueden utilizarse para extraer conclusiones precisas sobre la vida privada de los afectados, en particular sus perfiles de contactos e intereses. El problema de esta retención de metadatos se agrava considerablemente si autoridades policiales extranjeras también obtienen acceso directo a dicha información») (Datenschutzkonferenz, 2018).

Recientemente conocimos un ejemplo actual: tras destaparse el escándalo de presunta corrupción del secretario de organización del PSOE y ministro de Fomento, así como de Transportes, Movilidad y Agenda Urbana, José Luis *Ábalos* Meco (Miranda, 2024; Alonso, 2024), la ministra de Hacienda y vicepresidenta primera del gobierno, María Jesús Montero Cuadrado (PSOE) utilizó en el debate público las especulaciones sobre supuestas faltas fiscales de la pareja de la presidenta de la Comunidad de Madrid, Isabel Díaz Ayuso (PP), para desviar el foco de atención del PSOE (Benito, 2024; Sarriá, 2024; García, 2024). Se trataba de una información que la ministra no estaba legalmente autorizada a disponer ni a publicar. Es fácil imaginar los peligros que entraña la normativa sobre pruebas electrónicas, sobre todo para los países que se están alejando cada vez más de los principios democráticos.

Algunas consideraciones finales

La persecución de delincuentes en el espacio digital es una importante cuestión de interés. En particular, ahora que internet y los canales de comunicación asociados desempeñan un papel cada vez más importante en la preparación, ejecución y seguimiento de delitos violentos y actos de terrorismo en todo el mundo, las autoridades policiales y judiciales deben disponer de herramientas eficaces y eficientes para proteger la seguridad de todos nosotros de la mejor manera posible. Al mismo tiempo, deben defenderse los principios del Estado de Derecho. Existe, por tanto, un conflicto de objetivos entre la seguridad absoluta de los derechos individuales de los presuntos delincuentes y los del resto de la población, que debe ser protegida por el Estado de Derecho. En consecuencia, este conflicto de objetivos, esta zona de tensión, debe conciliarse de la mejor manera posible, y si esto se logrará con el Reglamento *E-Evidence* está por ver y dependerá también en gran medida de cómo utilicen las autoridades policiales y judiciales de los Estados miembros las nuevas posibilidades y en qué dirección se desarrollen las negociaciones entre la UE y los EE. UU. Lo que sí es seguro es que la aplicación del Reglamento *E-Evidence* debe ir acompañada de un proceso de evaluación crítica. En la medida de lo posible, debe evitarse el uso indebido de las competencias y, en caso de duda, el reglamento debe corregirse a tiempo.

Referencias bibliográficas

Abraha, H. (2020). Regulating law enforcement access to electronic evidence across borders: the United States approach. *Information & Communication Technology Law* (3), 324-353.

Alonso, M. (2024). Ábalos, el leal sanchista caído en desgracia. *ABC España*. https://www.abc.es/espana/abalos-leal-sanchista-caido-desgracia-20240225172744-nt.html.

Andreeva, C. (2020). The EU's counter-terrorism policy after 2015 — «Europe wasn't ready» — «but it has proven that it's adaptable». *ERA Forum* (20), 343-370.

Benito, M. (2024). La pareja de Ayuso se querellará contra la ministra Montero. *La Razón*. https://www.larazon.es/madrid/pareja-ayuso-querellara-ministra-montero_2024031565f44301ab79d80001a570a2.html.

Burchard, C. (2018). Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 1. *Zeitschrift für Internationale Strafrechtsdogmatik* (6), 190-203.

Commission Services. (2017). *Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward*. https://era-comm.eu/EPPO/kiosk/pdf/Non_paper_Improving_cross_border_access_electronic_evidence.pdf.

Consejo de la Unión Europea. (2016). *Council conclusions on improving criminal justice in cyberspace*. https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf.

Datenschutzkonferenz. (2018). *Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Münster, 7.* https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/DSK_20181107_EntschliessungE_Evidence.pdf?__blob=publicationFile&v=7.

De Hoyos Sancho, M. (2020). Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo. *Revista de Estudios Europeos* (1-extra), 99-128.

García, C. (2024). El PP denuncia las maniobras del sanchismo para desviar a Madrid la atención del «caso Koldo». *La Razón*. https://www.larazon.es/madrid/denuncia-maniobras-sanchismo-desviar-madrid-atencion-caso-koldo_2024030265e289ca566e5f00019e99f2.html.

Gora, A., De Wilde, P. (2020). The essence of democratic backsliding in the European Union: deliberation and rule of law. *Journal of European Public Policy* (2), 342-362.

Hay Derecho. (2023). *Situación del Estado de Derecho en España 2023*. https://www.hayderecho.com/wp-content/uploads/2023/12/Situacion-Estado-de-Derecho-Espana-2023.pdf.

López Werner, E. (2023). La exportación del terrorismo a través de Emni: un repaso de los atentados desde Siria hasta Libia, instrumentados bajo la marca del servicio de operaciones exteriores de Estado Islámico entre 2014 y 2017. *Revista del Instituto Español de Estudios Estratégicos* (21), c139-167.

Magno, T. (2023). The Challenging Path Towards the Establishment of the EU Legal Framework Regulating Cross-Border Access to Digital Evidence. En A. Biasiotti, F. Turchi (Coords.), *European Investigation Order* (23-33).

Martínez Santos, A. (2022). Emisión de órdenes europeas de investigación por el Ministerio Fiscal español. Consideraciones sobre la compatibilidad del art. 13.4 de la Ley de reconocimiento mutuo con el derecho de la Unión a la luz de las Sentencias del TJUE en los Asuntos Gavanozov I y II. *Revista General de Derecho Europeo* (57), 272-317.

Meissner, P. (2023). Digitale Beweise im EU-/US-Datenschutzkonflikt. *Verfassungsblog*. https://verfassungsblog.de/digitale-beweise-im-eu-us-datenschutzkonflikt/.

Miranda, B., (2024). José Luis Ábalos: simpático, mujeriego y prolífico. *El Mundo*. https://www.elmundo.es/loc/famosos/2024/02/22/65d729e5fc6c83fe068b4596.html.

Muriel Diéguez, J. (2024). Las Órdenes de Entrega y Conservación de Pruebas Electrónicas en el Proceso Penal Europeo. *Revista de Estudios Europeos* (83), 172-201.

Oromí i Vall-Llovera, S. (2020). Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE. *Revista de Internet, Derecho y Política* (31), 1-13.

Pacelli, D. (2023). El papel del miedo en los fenómenos colectivos: El miedo a los demás y la necesidad de la sociedad entre la política y la información. *Comunicación y Hombre* (19), 27-38.

Parlamento Europeo. (2023). *Electronic evidence: new rules to speed up cross-border criminal investigations*. https://www.europarl.europa.eu/news/es/press-room/20230609IPR96203/electronic-evidence-new-rules-to-speed-up-cross-border-criminal-investigations.

Raebisch, M. (2024). Pegasus: análisis de su impacto en los derechos fundamentales en Europa. *Quaderns IEE: Revista de l'Institut d'Estudis Europeus* (1), 62-87.

Robinson, G. (2023). Like Oil and Water? Effective Data Protection and Direct Cooperation on Digital Evidence. En V. Franssen, S. Tosza (Coords.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (1-35). Cambridge.

Ruíz Bursón, F. (2023). ¿Es constitucional una ley de amnistía? Estado actual de la cuestión: argumentos a favor y en contra. *Corts. Anuari de Dret Parlamentari* (37), 83-127.

Sarriá, B. (2024). Génova respalda a Ayuso ante el señalamiento del PSOE por las cuentas de su pareja: «No afecta al PP». *20minutos*. https://www.20minutos.es/noticia/5227072/0/genova-respalda-ayuso-ante-senalamiento-psoe-por-las-cuentas-su-novio-no-afecta-pp/.

Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679.

Unión Europea. (2017). *Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se*

modifica la Decisión 2005/671/JAI del Consejo. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32017L0541.

Unión Europea. (2023a). *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.* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32023L1544.

Unión Europea. (2023b). *Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales.* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32023R1543.

US Department of Justice. (2018). *Clarifying Lawful Overseas Use of Data Act.* https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf.

Villoria Mendieta, M. (2022). Un análisis comparado de la lucha contra la corrupción en Europa, con especial referencia a España. *Revista Española de Control Externo* (72) 10-35.