diariolaley

Prueba digital internacional. El Reglamento E-Evidence

Joaquín Delgado Martín
Magistrado Sala Penal Audiencia Nacional. Doctor en Derecho
Miembro de la REDUE (Red de Expertos en Derecho Europeo)

Diario LA LEY, Nº 76, Sección Ciberderecho, 15 de Septiembre de 2023, **LA LEY**

ÍNDICE

Normativa comentada

TUE 7 Feb. 1992 (Tratado Maastricht)
TÍTULO V.. DISPOSICIONES GENERALES RELATIVAS A LA ACCIÓN EXTERIOR DE LA UNIÓN Y DISPOSICIONES ESPECÍFICAS RELATIVAS A LA POLÍTICA EXTERIOR Y DE SEGURIDAD COMÚN
CAPÍTULO 2. DISPOSICIONES ESPECÍFICAS SOBRE LA POLÍTICA EXTERIOR Y DE SEGURIDAD COMÚN
SECCIÓN 1. DISPOSICIONES COMUNES
Artículo 34.
Regl. 2023/1543 UE, de 12 Jul. (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)
Directiva 2017/541 UE, de 15 Mar. (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)
TÍTULO II. DELITOS DE TERRORISMO Y DELITOS RELACIONADOS CON UN GRUPO TERRORISTA
Artículo 3. *Delitos de terrorismo*

Comentarios

Resumen

Dado el exponencial aumento del volumen de datos generados en los últimos años, y su tendencia a multiplicarse de forma muy acelerada como consecuencia de avances tecnológicos, se ven muy incrementadas las posibilidades de investigación del delito mediante la obtención y análisis de los datos generados que se encuentran en poder de los proveedores, pero, a la vez, también aumenta las dificultades de ser abordados por los órganos de investigación penal. En este marco resulta relevante la necesidad de unos instrumentos que faciliten la obtención de esas pruebas, por medio de una adecuada colaboración, tanto judicial como público-privada, es decir, de las autoridades públicas con las empresas tecnológicas.

1. Prueba digital internacional: datos en poder de proveedores

1.1. Relevancia

El acceso a los datos en poder de los proveedores o prestadores de servicios constituye actualmente un **elemento esencial para la investigación de todo tipo de delitos**, y también para **asegurar el cumplimiento del ordenamiento jurídico en el ciberespacio**. Alexander SEGER considera que «*la obtención de pruebas electrónicas para su uso en procesos penales es esencial para el Estado de Derecho*»; y añade que «*la capacidad de los gobiernos para garantizar el estado de derecho en el ciberespacio seguirá siendo limitada, a menos que se puedan superar los impedimentos para acceder a datos y, por lo tanto, a pruebas electrónicas para la justicia penal. La falta de datos significa que no hay prueba, que no hay justicia, y por tanto la falta de estado de derecho*» (1) .

Téngase en cuenta que el volumen de datos (2) se ha incrementado de forma masiva en los últimos años (3) , y la tendencia es a multiplicarse de forma muy acelerada como consecuencia de avances tecnológicos ligados al IOT (Internet de las Cosas), Botnets, 5G, computación cuántica, AI (Inteligencia Artificial), entre otros. Según el Global Data Protection Index 2020 Snapshot (4) , elaborado por The Dell Technologies, las organizaciones administran actualmente 13.53 petabytes (PB) de datos, lo que supone casi un 40% de aumento frente a los 9.70 PB en 2018, y un aumento del 831% frente a los 1.45 PB en 2016. Un petabyte es una unidad de almacenamiento de información que equivale a 1.000.000.000.000.000 de bytes (5) . Ello incrementa las posibilidades de investigación del delito mediante la obtención y análisis de los datos generados que se encuentran en poder de los proveedores, pero también aumenta las dificultades de ser abordados por los órganos de investigación penal. En este marco resulta relevante abordar una colaboración adecuada público-privada, es decir, de las autoridades públicas con las empresas tecnológicas.

El Informe de Impacto que acompaña a la Propuesta de Reglamento E-Evidence (6) recoge una estimación del porcentaje de investigaciones penales que incluyen una solicitud de datos transfronteriza:

- La evidencia electrónica en cualquier forma es relevante en alrededor del 85% del total de las investigaciones (penales).
- En casi dos tercios (65%) de las investigaciones en las que la evidencia electrónica es relevante, se necesita una solicitud a los proveedores de servicios transfronterizos (con sede en otra jurisdicción).
- La combinación de los dos porcentajes anteriores da como resultado el 55% del total de las investigaciones incluyen una solicitud de acceso transfronterizo a la evidencia electrónica.
- Las solicitudes de datos sin contenido superan en número a las de contenido dentro de la UE y más allá. Los datos sin contenido de las comunicaciones electrónicas se solicitan con mayor frecuencia.
- Sin embargo, se cumplimentan menos de la mitad de todas las solicitudes a los proveedores de servicios.

1.2. Dificultades en la obtención de datos en poder de los proveedores de servicios

1.2.1. Peligro de pérdida de datos

Existe una volatilidad de los datos en poder de los proveedores de servicio, que se deriva de dos elementos: muchos Estados no tienen normativa que obligue a la retención de datos para la investigación penal; y los requisitos de minimización de datos obligan a los proveedores a eliminar datos más rápidamente (protección de datos personales). Y la pérdida de datos también se relaciona con los desafíos relacionados con la gobernanza de Internet, la encriptación de comunicaciones, y el uso de criptomonedas (7) .

1.2.2. Localización de los datos

Frecuentemente resulta difícil conocer la ubicación de la infraestructura del grupo criminal o del autor del delito, y/o la propia localización de los datos; lo que se complica cuando los investigados utilizan instrumentos de encriptación y/o anonimización de sus comunicaciones, las criptomonedas y la Dark Web; téngase en cuenta que éstos van perfeccionando sus medidas de seguridad y adaptando su «modelo de negocio ilícito» a los avances tecnológicos y al resultado exitoso de investigaciones policiales. En estos casos será complicado establecer la concreta jurisdicción competente y el régimen jurídico aplicable para la obtención de los datos mediante medidas de investigación tecnológica.

1.2.3. Falta de un marco legal adecuado

En primer lugar, a menudo concurre una insuficiencia de los ordenamientos nacionales, así como diferencias entre los mismos; así como un diferente tratamiento legal de la retención y acceso a los datos en los diferentes países, o incluso una falta de legislación nacional que lo regule.

En segundo lugar, la ausencia de instrumentos normativos internacionales adecuado contribuye a dificultar la utilización de los datos en poder de proveedores para la investigación y prueba de los delitos; sin perjuicio de los avances que se han dado últimamente: Segundo Protocolo del Convenio de Budapest; y Reglamento E-evidence. En este sentido, el apartado 8 del Preámbulo del Reglamento E-evidence afirma que «*…no existe un marco armonizado para la cooperación con los prestadores de servicios, mientras que algunos prestadores de terceros países aceptan solicitudes directas de datos que no sean datos de contenido si lo permite su Derecho nacional aplicable. Por ello, los Estados miembros dependen cada vez más de los canales de cooperación voluntaria y directa con los prestadores de servicios cuando se disponga de ellos, y aplican diferentes instrumentos, condiciones y procedimientos nacionales. Para los datos de contenido, algunos Estados miembros han adoptado medidas unilaterales, mientras que otros siguen confiando en la cooperación judicial*». Y su apartado 9 añade que «*la fragmentación del marco jurídico supone una dificultad para las autoridades policiales y las autoridades judiciales, así como para los prestadores de servicios que desean cumplir los requerimientos judiciales de pruebas electrónicas, ya que se enfrentan cada vez más a una inseguridad jurídica y, potencialmente, a conflictos de leyes*»

Resulta especialmente relevante la utilización de las estructuras de colaboración entre autoridades judiciales y policiales de diferentes países

En este marco resulta especialmente relevante la utilización de las estructuras de colaboración entre autoridades judiciales y policiales de diferentes países, es decir, los instrumentos de cooperación policial y judicial internacional, tanto a nivel regulatorio (normas de cooperación o asistencia internacional) como institucional (instituciones, redes y otros foros de asistencia e intercambio de información y experiencias).

1.2.4. Desafíos de las novedades tecnológicas

Muchos proveedores utilizan la **encriptación** para sus servicios, frecuentemente de manera predeterminada, permitiendo el cifrado personal y el anonimato de las comunicaciones. Constituye un elemento esencial en la sociedad digitalizada, ayudando a garantizar la protección de nuestros derechos humanos más fundamentales y a proteger la seguridad de nuestra economía digital; pero también es verdad que facilita oportunidades significativas para los delincuentes. En definitiva, dificulta la utilización de las medidas de investigación tecnológica, lo que resulta especialmente preocupante en materia de explotación sexual infantil o de terrorismo.

También existen obstáculos a la investigación que derivan de la utilización por los proveedores de la **tecnología Carrier-Grade Network Address Translation** (CGN o Carrier Grade NAT), que permite compartir una sola dirección IPv4 pública entre múltiples suscriptores (usuarios finales) al mismo tiempo (posiblemente varios miles). Se trata de una solución tecnológica utilizada por el 95% de los proveedores móviles (operadores de red y operadores de redes virtuales móviles) y cerca del 50% de los proveedores de servicios de Internet tradicionales (ISP: cable, fibra y ADSL) en todo el mundo. Téngase en cuenta que, para que los proveedores puedan identificar técnicamente a un usuario final tras un CGN basado en un IPv4 público, es necesario conocer una dirección IPv4, la hora precisa de conexión y el número de puerto de origen. Sin embargo, el número de puerto de origen no suele ser conservado por los proveedores de servicios electrónicos, las plataformas de redes sociales, los servicios de correoweb, los servicios de alojamiento de datos, etcétera; por lo que no se podrá individualizar al usuario final, sino que hay que investigar todos los usuarios asociados a esa dirección IPv4 (8) .

1.2.5. Dimensión internacional

Los proveedores de servicios almacenan los datos de los usuarios en uno o varios servidores, que pueden hallarse en distintos países tanto dentro como fuera de la UE. Se calcula que en más del 50 % de las investigaciones penales hay que cursar una solicitud de obtención de pruebas electrónicas (9) . En estos casos, el acceso a estos datos por los órganos del sistema penal resulta mucho más complejo, deviniendo lento y costoso, e incluso en ocasiones materialmente imposible.

1.2.6. Ineficiencias en la colaboración público-privada

También concurren desafíos de la colaboración público-privada, que se concreta en tres cuestiones: marco legal; definición de la jurisdicción competente; y retos asociados con las tecnologías nuevas y emergentes (10) . La inadecuación de esta colaboración puede tener efectos negativos sobre la investigación y prueba de los ciberdelitos.

2. Instrumentos para la obtención de datos en poder de proveedores

2.1. Cooperación o asistencia judicial internacional

Una primera forma de obtener datos en poder de proveedores radicados fuera del territorio nacional consiste en acudir a la Comisión Rogatoria Internacional (instrumento formal de asistencia judicial internacional o Mutual Legal Assistance-MLA) cumplimentada y remitida de conformidad con el instrumento legal aplicable (convenio internacional bilateral o multilateral, o bien Orden de Europea de Investigación en la UE).

Sin embargo, la práctica demuestra la gran dificultad de acudir a este tipo de asistencia. Los esquemas clásicos de la cooperación judicial internacional se muestran ineficaces en una parte importante de los supuestos. Y también en el ámbito de la UE: como afirma el propio Preámbulo del Reglamento E-evidence, «*…los procedimientos y plazos previstos en la Directiva 2014/41/UE (LA LEY 6702/2014) relativa a la OEI y en el Convenio relativo a la asistencia judicial en materia penal podrían no ser adecuados para las pruebas electrónicas, que son más volátiles y podrían eliminarse con mayor facilidad y rapidez. La obtención de pruebas electrónicas utilizando los canales de cooperación judicial a menudo lleva mucho tiempo, lo que da lugar a situaciones en las que los indicios podrían no estar ya disponibles*» (apartado 8).

2.2. Entrega voluntaria por el proveedor de servicios

Frente a estas dificultades de la cooperación judicial, se suele acudir a la entrega voluntaria por el proveedor de servicios: algunos proveedores aceptan solicitudes de datos que son remitidas directamente por la policía y las autoridades judiciales de otros países.

Es necesario tener presente que el concreto proveedor de servicios requerido

El concreto proveedor de servicios requerido entregará los datos solicitados con sometimiento a su política interna, es decir, conforme a sus propias reglas de funcionamiento

entregará los datos solicitados con **sometimiento a su política interna**, es decir, conforme a sus propias reglas de funcionamiento. Por ejemplo, Facebook puede revelar al agente autorizado una cantidad limitada de información básica del suscriptor, según cada caso (11) : número de identificación del usuario, dirección de correo electrónico, sello de la fecha y hora de creación de la cuenta en Tiempo universal coordinado (UTC), inicios de sesión más recientes, número de teléfono móvil registrado, información sobre si el perfil del usuario se ha indexado públicamente a través de motores de búsqueda; y también puede facilitar registros de IP. En relación con Gmail, Google solamente proporcionará: información de registro del suscriptor (por ejemplo, nombre, información de creación de cuenta, direcciones de correo electrónico asociadas, número de teléfono); direcciones IP de inicio de sesión y sellados de tiempo asociadas; e información no relacionada con contenido (como la información del encabezado del correo electrónico que no es contenido: el de y para, la hora de envío y la IP, con la línea del asunto eliminada). En relación con YouTube, Google proporciona: información de registro del suscriptor; direcciones IP de inicio de sesión y sellados de tiempo asociadas; y dirección IP de carga de video y sellado de tiempo asociada. Y Google ha comunicado que la Entidad prestadora de servicios en el Espacio Económico Europeo y Suiza es Google Ireland Limited, siendo la única entidad que tiene acceso y dispone de los datos que pueden ser requeridos en el ámbito de los procedimientos judiciales.

2.3. Nuevos instrumentos jurídicos: relación directa con los proveedores

2.3.1. Segundo Protocolo del Convenio de Budapest

El 12 de mayo de 2022 tuvo lugar en Estrasburgo la firma por 22 Estados, incluido España, del Segundo Protocolo Adicional a la Convención sobre la Cibercriminalidad relativo al reforzamiento de la cooperación y de la entrega de pruebas electrónicas. De esta forma, queda abierto el proceso de ratificación por parte de los países, de tal manera que el convenio entrará en vigor cuando se ratifique por cinco Estados (12) . En este sentido, el Consejo de la Unión Europea ha adoptado con fecha 5 de abril de 2022 una decisión por la que se autoriza a los Estados miembros a firmar, en interés de la UE, el Segundo Protocolo Adicional.

Nos encontramos con una normativa que no es solamente aplicable a las investigaciones o **procedimientos penales específicos por delitos relativos a datos y sistemas informáticos**, sino también a la **obtención de pruebas digitales sobre cualquier delito** —no solamente en materia de cibercriminalidad— (artículo 2.1 del Segundo Protocolo).

En el presente trabajo cabe destacar la primera parte del Segundo Protocolo, que se refiere a una serie de **medidas de cooperación reforzada en relación con datos informáticos almacenados** en otro Estado (13) :

- Procedimientos que mejoran la cooperación directa con proveedores y entidades que prestan servicio en el territorio de otro Estado parte. El Segundo Protocolo establece mecanismos que permitan la relación directa entre la autoridad penal competente de un Estado y el proveedor que presta servicio en el territorio de otro Estado parte: informaciones para identificar o contactar a la persona que registró un nombre de dominio (artículo 6); y para acceso a datos relativos a los abonados (artículo 7)
- Procedimientos que mejoran la cooperación internacional entre autoridades para la entrega de datos informáticos almacenados: para dar efecto a los mandatos judiciales de otra Parte que ordenan la entrega acelerada de información sobre abonados y datos de tráfico (artículo 8); así como para la entrega acelerada de datos informáticos almacenados específicos en caso de urgencia (artículo 9)

Este Segundo Protocolo también cuenta con una segunda parte que regula con carácter general determinados aspectos de la asistencia judicial urgente (artículo 10); así como una tercera parte que contempla dos instrumentos de cooperación internacional específicos en caso de ausencia de convenios internacionales aplicables: la regulación de la videoconferencia (artículo 11) y los equipos conjuntos de investigación e investigaciones comunes (artículo 12).

2.3.2. Nuevo sistema en la UE: sistema E-Evidence

El Diario Oficial de la Unión Europea del 28 de julio ha publicado dos instrumentos que diseñan un nuevo sistema, cuyo elemento esencial radica en que la autoridad judicial del Estado emisor puede **remitir directamente la solicitud**

al proveedor de servicios situado en cualquier Estado de la Unión Europea, en concreto al representante que dicho proveedor haya designado a estos efectos, con el criterio inspirador del principio de reconocimiento mutuo (14) .

A. El **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.

- Este Reglamento **será aplicable a partir del 18 de agosto de 2026**. No obstante, la obligación de las autoridades competentes y los prestadores de servicios de utilizar el sistema informático descentralizado establecido en el artículo 19 para la comunicación escrita en virtud del presente Reglamento se aplicará a partir de un año después de la adopción de los actos de ejecución a que se refiere el artículo 25.

B. La **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.

- Los establecimientos designados y los representantes legales previstos en esta Directiva deben servir de destinatarios de las resoluciones y órdenes a efectos de recabar pruebas electrónicas sobre la base del Reglamento (UE) 2023/1543 (LA LEY 22209/2023) (E-evidence), de la Directiva 2014/41/UE (LA LEY 6702/2014) del Parlamento Europeo y del Consejo (orden europea de investigación en materia penal) y del Convenio celebrado por el Consejo, de conformidad con el artículo 34 del Tratado de la Unión Europea (LA LEY 109/1994), relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea (7), también cuando dichas resoluciones y órdenes se transmitan en forma de certificado. Y también se aplica a las resoluciones y órdenes a efectos de recabar pruebas electrónicas sobre la base del Derecho nacional dirigidas por un Estado miembro a una persona física o jurídica que actúe como representante legal o como establecimiento designado de un prestador de servicios en el territorio de dicho Estado miembro.
- Plazo de transposición. Los Estados miembros pondrán en vigor a más tardar el **18 de febrero de 2026** las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones.

El panorama normativo de la UE en este ámbito puede sistematizarse de la siguiente forma:

UNIÓN EUROPEA	VIGENTE	TRAS 2026
INTERVENCIÓN COMUNICACIONES	Orden Europea de Investigación (específica)	Orden Europea de Investigación (específica)
PRESERVACIÓN DATOS	Orden Europea de Investigación (genérica)	Orden Europea de Conservación-EPOC-PR (Reglamento E-evidence)
REMISIÓN DATOS	Orden Europea de Investigación (genérica)	Orden Europea de Producción-EPOC (Reglamento E-evidence)

3. Sobre el reglamento e-evidence

3.1. Ámbito de aplicación

3.1.1. ¿Cuál es el objeto?

- La entrega o conservación de una **prueba electrónica para un proceso penal**. La autoridad competente de un Estado puede solicitar una actuación sobre determinados datos en formato electrónico (de los abonados, datos de tráfico o datos de contenido) directamente a un prestador de servicios que los tiene almacenados: bien la entrega de esos datos para que surtan efecto en un proceso penal (**Orden Europea de Producción**-EPOC-European Production Order Certificate), o bien su conservación a efectos de solicitar su posterior entrega (**Orden Europea de Conservación**-EPOC-PR-European Preservation Order Certificate).
- Sin perjuicio de las normas de cooperación judicial internacional o de asistencia judicial entre Estados

miembros de la UE

3.1.2. ¿Qué datos pueden ser objeto de una Orden?

No hay que olvidar que los datos conservados por los proveedores no suponen el mismo **grado de afectación de los derechos fundamentales**. En este sentido resulta relevante lo que hemos denominado «la fórmula de la proporcionalidad» (15) : cuanto mayor sea la limitación del derecho fundamental afectado, mayor ha de ser el interés tenido en cuenta para justificar la intervención estatal en el caso concreto (16) ; y una más grande intensidad en la vulneración del derecho fundamental exige que el Juez extreme el celo en el examen y motivación de la concurrencia de los elementos descritos a la hora de exponer el juicio de proporcionalidad.

Este diferente grado de afectación despliega efectos no solamente sobre la valoración que ha de efectuar la autoridad autorizante en torno el juicio de proporcionalidad; sino también sobre el propio régimen jurídico del Reglamento E-evidence, siendo más estricto para los datos de tráfico y los datos de contenido (ámbito objetivo, autoridad competente para la emisión…). En este sentido, el Reglamento establece que la obtención de datos de los abonados o de datos solicitados con el único fin de identificar al usuario puede ser también acordado por el fiscal.

A.- Dimensión objetiva 1.- ¿Qué modalidades de datos?

- **Datos de los abonados**: cualesquiera datos que obren en poder de un prestador de servicios relativo a la suscripción a sus servicios, en relación con

  a) la identidad del abonado o cliente, como nombre, fecha de nacimiento, dirección postal o geográfica, facturación y pagos, número de teléfono o dirección de correo electrónico;
  b) 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;

- **Datos solicitados con el único fin de identificar al usuario**: las direcciones IP y, cuando sea necesario, los puertos de origen y el sello de tiempo pertinentes, a saber, la fecha y la hora o equivalentes técnicos de dichos identificadores e información conexa, cuando así lo soliciten las autoridades policiales o las autoridades judiciales con el único fin de identificar al usuario en una investigación penal específica;
- **Datos de tráfico**: los datos relacionados con la prestación de un servicio ofrecido por un prestador de servicios que sirvan para facilitar información contextual o adicional sobre dicho servicio y sean generados o tratados por un sistema de información del prestador de servicios, tales como el origen y destino de un mensaje u otro tipo de interacción, 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 al servicio y la desconexión del servicio;
- **Datos de contenido**: cualesquiera datos en formato digital, como texto, voz, vídeos, imágenes y sonidos, que no sean datos de abonados o datos de tráfico

B.- Dimensión objetiva 2.- ¿Para qué procesos penales?

Las órdenes europeas pueden emitirse en el seno de un **proceso penal**. Sin embargo, no pueden emitirse por cualquier **delito,** sino que su concreto ámbito dependerá del tipo de datos solicitados:

- **Datos de los abonados o datos solicitados con el único fin de identificar al usuario**

  - para todas las infracciones penales
  - y para fines de ejecución de una pena o de una medida de seguridad privativas de libertad de al menos cuatro meses, tras un proceso penal, impuestas por una resolución que no se haya dictado en rebeldía, en los casos en que la persona condenada haya huido de la justicia.

- **Datos de tráfico o datos de contenido**

  - Para las infracciones penales punibles en el Estado emisor con una pena máxima privativa de libertad de al menos tres años, o específicas infracciones penales (que enumera por remisión a otras Directivas), siempre que hayan sido cometidas total o parcialmente por medio de un sistema de información
  - Para las infracciones penales definidas en los artículos 3 a (LA LEY 4537/2017)12 (LA LEY 4537/2017) y 14 de la Directiva (UE) 2017/541 (LA LEY 4537/2017) relativa a la lucha contra el terrorismo;
  - Para la ejecución de una pena o de una medida de seguridad privativas de libertad de al menos cuatro meses a raíz de un proceso penal, impuestas por una resolución que no se haya dictado en rebeldía, en los casos en que la persona condenada haya huido de la justicia, por infracciones penales a que se refieren las letras a), b) y c) del presente apartado.

C.- Dimensión temporal

- La Orden puede referirse a datos **almacenados en el momento en que se reciba la Orden**
- El Reglamento no contempla una obligación general de retención de datos por parte de los prestadores de servicios;
- Ni tampoco puede aplicarse a otros datos almacenados tras la recepción de la Orden

D.- Dimensión subjetiva. ¿Qué entidades tienen la obligación de cumplir estas órdenes?

- **Proveedores de servicios de comunicaciones electrónicas**: los prestados por lo general a cambio de una remuneración a través de redes de comunicaciones electrónicas, que incluye, con la excepción de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos, los siguientes tipos de servicios:

  - el servicio de acceso a internet
  - el servicio de comunicaciones interpersonales
  - Y los servicios consistentes, en su totalidad o principalmente, en el transporte de señales, como son los servicios de transmisión utilizados para la prestación de servicios máquina a máquina y para la radiodifusión

- **Proveedores de infraestructura de internet**

  - Proveen 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

- **Prestadores de otros servicios de la sociedad de la información determinados**: todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios; siempre que:

  - Permitan a sus usuarios comunicarse entre sí,
  - O permitan almacenar o tratar datos de otro modo en nombre de los usuarios a los que se presta el servicio, siempre que el almacenamiento de datos sea un componente esencial del servicio prestado al usuario;

E.- Dimensión territorial

- Un prestador que **ofrezca servicios en la Unión**

  a) Permitir que personas físicas o jurídicas en un Estado miembro utilicen los servicios enumerados en el punto 3, y
  b) tener una conexión sustancial, basada en criterios fácticos específicos, con el Estado

miembro a que se refiere la letra a); debe considerarse que existe tal conexión sustancial cuando el prestador de servicios disponga de un establecimiento en un Estado miembro o, en ausencia tal establecimiento, cuando exista un número significativo de usuarios en uno o más Estados miembros, o se orienten actividades hacia uno o más Estados miembros;

- Y establecido o representado en otro Estado miembro de la UE:
  - Que esté **establecido** en otro Estado miembro
  - O que no está establecido en otro Estado miembro, pero que esté r**epresentado** por un representante legal en otro Estado miembro,

3.2. Emisión de la Orden

3.2.1. ¿Qué autoridades pueden emitir las órdenes?

Como hemos analizado anteriormente, depende de la mayor o menor afectación a los derechos fundamentales de los datos objeto de la Orden.

- Datos de tráfico o datos de contenido
  - Un **juez, tribunal o juez de instrucción** competente en el asunto de que se trate, o
  - cualquier otra autoridad competente, según la defina el Estado emisor que, en el asunto de que se trate, actúe en calidad de **autoridad de investigación** en procesos penales y tenga competencia para ordenar la obtención de pruebas de conformidad con el Derecho nacional; en tal caso, la orden europea de producción será **validada**, previo examen de su cumplimiento de las condiciones de emisión en virtud del presente Reglamento, por un juez, tribunal o juez de instrucción del Estado emisor
- Datos de los abonados o datos solicitados con el único fin de identificar al usuario
  - Además de los anteriores, el **fiscal** competente en el asunto de que se trate.

3.2.2. ¿Cuál es la forma de emisión?

- Mediante la remisión de un **certificado**
  - EPOC: anexo I
  - EPOC-PR: anexo II

3.2.3. ¿Cuál es la forma de remisión?

- **Remisión directa**
  - Se dirigirán directamente al establecimiento designado o a un representante legal del prestador de servicios afectado (artículo 7.1)
  - Excepcionalmente, en los casos urgentes definidos en el artículo 3, punto 18, cuando el establecimiento designado o el representante legal de un prestador de servicios no reaccione ante un EPOC o un EPOC-PR en los plazos establecidos, dicho EPOC o EPOC-PR podrá dirigirse a cualquier otro establecimiento o representante legal del prestador de servicios en la Unión (artículo 7.2)

3.3. Ejecución de la Orden

3.3.1. Orden de Conservación

- Una vez recibido un EPOC-PR, el destinatario conservará, **sin demora** indebida, los datos solicitados.
- La obligación de conservar los datos cesará transcurridos **60 días**, a menos que la autoridad emisora confirme, utilizando el formulario que figura en el anexo V, que se ha emitido una solicitud posterior de entrega.

- Durante ese período de 60 días, la autoridad emisora podrá, utilizando el formulario que figura en el anexo VI, prorrogar la duración de la obligación de conservar los datos por un período adicional de 30 días, cuando sea necesario para permitir la emisión de una solicitud posterior de entrega

3.3.2. Orden de Producción

- **Contestación**
  - Entrega de datos
  - O bien comunicación de un motivo de denegación
- **Plazo de contestación**
  - Lo antes posible, y a más tardar en un plazo de **diez días** a partir de la recepción de la notificación,
  - En casos urgentes, a más tardar en un plazo de **96 horas** a partir de dicha recepción,
- **Motivos de denegación**
  - Los datos solicitados están protegidos por **inmunidades o privilegios** concedidos en virtud del Derecho del Estado de ejecución que impidan la ejecución de la orden, o los datos solicitados están cubiertos por normas sobre la determinación o limitación de la responsabilidad penal relacionadas con la **libertad de prensa o la libertad de expresión** en otros medios de comunicación que impidan la ejecución de la orden;
  - En situaciones excepcionales, existen motivos fundados para suponer, sobre la base de pruebas concretas y objetivas, que la ejecución de la orden conllevaría, en las circunstancias particulares del caso, una **vulneración manifiesta de un derecho fundamental** pertinente establecido en el artículo 6 del TUE y en la Carta;
  - La ejecución de la orden sería contraria al **principio *non bis in idem***;
  - La conducta que dio origen a la emisión de la orden **no es constitutiva de infracción penal** con arreglo al Derecho del Estado de ejecución, y no está recogida en las categorías de delitos que figuran en el anexo IV, conforme a lo indicado por la autoridad emisora en el EPOC, si en el Estado emisor es punible con una pena o una medida de seguridad privativas de libertad de una duración máxima no inferior a tres años.

(1) Alexander SEGER «Evidence in the cloud and the rule of law in cyberspace: avoiding the "jungle"». https://www.friendsofeurope.org/insights/evidence-in-the-cloud-and-the-rule-of-law-in-cyberspace-avoiding-the-jungle/

(2) El Volumen (cantidades masivas de datos que se generan y se almacenan con la finalidad de procesar dicha información) es una de las 7 V del Big Data: Volumen, Velocidad, Variedad de los datos, Veracidad de los datos, Viabilidad, Visualización de los datos y Valor de los datos. Véase un resumen en el blog https://www.iic.uam.es/innovacion/big-data-caracteristicas-mas-importantes-7-v/

(3) IBM estimó en 2017 que el 90% de los datos mundiales se habían creado en los últimos dos años; Julián Torres Santeli, Sabine Gerdon. World Economic Forum, «5 challenges for government adoption of AI», 16 de agosto de 2019; https://www.weforum.org/agenda/2019/08/artificial-intelligence-government-public-sector

(4) https://www.delltechnologies.com/en-us/data-protection/gdpi/index.htm#gdpi_2020

(5) Cambridge Dictionay, https://dictionary.cambridge.org/es/diccionario/ingles/petabyte

(6) Informe de Impacto que acompaña a la Propuesta de Reglamento E-Evidence de 17 de abril de 2018 SWD(2018) 118 final; página 14 https://eur-*lex*.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN

(7) EUROJUST-EUROPOL, «Common challenges in combating cybercrime as identified by Eurojust and Europol», June 2019; https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime

(8) EUROJUST-EUROPOL, «Common challenges in combating…»

(9) https://www.consilium.europa.eu/es/policies/e-evidence/

(10) EUROJUST-EUROPOL, «Common challenges in combating cybercrime…»

(11) «Directrices de Facebook para las autoridades encargadas del cumplimiento de la ley», disponible en el Prontuario de Asistencia Judicial Internacional [www.prontuario.org]

(12) En el momento de redacción de este trabajo, lo han firmado 40 Estados; aunque solamente consta ratificado por Serbia y por Japón.

(13) Véase mi trabajo sobre «Presente y futuro de la prueba digital internacional. El Segundo Protocolo Adicional del Convenio de Budapest contra la cibercriminalidad», Diario La Ley, N.º 62, Sección Ciberderecho, 24 de mayo de 2022.

(14) Olga FUENTES SORIANO, «Europa ante el reto de la prueba digital. El establecimiento de instrumentos probatorios comunes: las órdenes europeas de entrega y conservación de pruebas electrónicas», dentro de la obra *Era digital, sociedad y Derecho*, editorial Tirant lo Blanch, 2020, páginas 281 y ss.

(15) Véanse mis trabajos sobre «Intervenciones corporales. Su colisión con los derechos fundamentales», publicado en la revista *Iuris*, n.º 55, noviembre 2001, página 68; y «La resolución judicial de entrada y registro en lugar cerrado», *Actualidad Penal*, n.º 47, 17 a 23 de diciembre de 2001, página 1.133.

(16) Como dice Nicolás GONZÁLEZ-CUELLAR SERRANO, el interés de la persecución penal *«ha de ser más alto cuanto más graves las medidas»,* en *La proporcionalidad y derechos fundamentales en el proceso penal*, editorial Colex, Madrid, página 309.