



**Cooperación
Española**

CONOCIMIENTO / INTERCOONECTA

Curso de Especialización Judicial
“Ciberdelincuencia: tratamiento preventivo, procesal y
sustantivo desde una perspectiva internacional”. 4ª
Edición

4.1.- PROBLEMÁTICA TRANSNACIONAL Y COOPERACIÓN PENAL INTERNACIONAL

Autor

Joaquín Delgado Martín

Magistrado Sala Penal de la Audiencia Nacional

ESPAÑA



ESQUEMA GENERAL DE LA INTERVENCIÓN:

1. Prueba digital internacional

- a. ¿Qué puede solicitarse a las autoridades extranjeras?**
- b. Sistema del Convenio de Budapest**
- c. Sistema del Tratado de Madrid**
- d. Sistema de la Unión Europea**

2.- Datos en poder de proveedores de servicios situados fuera del territorio nacional

- a. Estrategia y Decálogo de recomendaciones**
- b. Proveedor situado en USA**
- c. Panorama de futuro**

1.- PRUEBA DIGITAL INTERNACIONAL





- **PRUEBA DIGITAL: ¿QUÉ PUEDE SOLICITARSE A LAS AUTORIDADES EXTRANJERAS?**

1. OBTENCIÓN DATOS EN TIEMPO REAL EN UNA COMUNICACIÓN
2. REMISIÓN DE DATOS ALMACENADOS

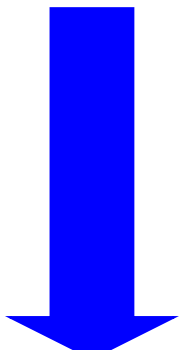
1.- PROCESO EN PAÍS REQUERENTE



2.- SOLICITUD A AUTORIDAD JUDICIAL EXTRANJERA



3.- ACTUACIÓN DE LA AUTORIDAD EXTRANJERA



4.- VALIDEZ EN PAÍS REQUERENTE DE LO ACTUADO

• PROCESO EN ESTADO REQUERENTE

- Necesidad resolución judicial admitiendo la prueba digital: normas nacionales

• SOLICITUD A LA AUTORIDAD EXTRANJERA

- Por Comisión Rogatoria Internacional (CRI): con fundamento en Convenio aplicable (bilateral o multilateral); o solicitud AJI

• ACTUACIÓN DE LA AUTORIDAD EXTRANJERA

- La intervención se realiza de conformidad con el ordenamiento interno del Estado requerido (*lex loci*): principio clásico de la cooperación internacional (art. 3.1 Convenio 59 y en principales Convenios bilaterales como EEUU 2004, Brasil 2006 y México 2006)
- UE: Orden Europea de Investigación permite que se solicite que se realice observando los trámites indicados expresamente por el Estado requerente

• VALOR EN ESTADO REQUERENTE DE LA PRUEBA OBTENIDA

- **VALOR EN PAIS REQUERENTE DE LA PRUEBA OBTENIDA**
(Jurisprudencia penal española)
 - Principio general:
 - *Validez: prueba obtenida en el extranjero conforme a las normas del país es válida en España*
 - *Valoración: por el tribunal de enjuiciamiento español de conformidad con las normas del ordenamiento español*
 - Cabe valorar si fue practicada conforme ley del país: la inobservancia ha de ser probada por quien lo alega
 - Cabe valorar también si en el país de ejecución se han mantenido unas garantías sustancialmente similares a las exigidas en España para la restricción de los derechos de los ciudadanos: para ello, es “preciso aportar un **dato objetivo sugestivo** de una posible infracción de derechos fundamentales no tolerable por nuestro ordenamiento” (STS 1099/2005); y debe ser alegado y probado por quien lo quiera hacer valer
 - UE: criterio general de confianza con fundamento en garantías comunes en el espacio judicial europeo

COOPERACIÓN JUDICIAL CIVIL:

Bilaterales+Multilaterales

Convenio de La Haya, de 18 de marzo de 1970, relativo a la obtención de pruebas en el extranjero en materia civil o mercantil

- **Página web de la Conferencia de la Haya (<http://www.hcch.net>)**



Convención Interamericana sobre exhortos o cartas rogatorias, hecho en Panamá el 30 de enero de 1975

- **Página web de la Organización de Estados Americanos (<http://www.oas.org/juridico/spanish>)**



UNIÓN EUROPEA: Reglamento (CE) 1206/2001 de 28 de mayo de 2001, relativo a la cooperación entre los órganos jurisdiccionales de los Estados miembros en el ámbito de la obtención de pruebas en materia civil o mercantil

COOPERACIÓN JUDICIAL PENAL

- Posible **Convenio bilateral**. Estos convenios no tienen normativa específica sobre prueba digital
- Posibles **Convenios multilaterales en materias específicas**. Destacables en materia penal:
 - Art. 18 Convenio Palermo (Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional 2000)
 - Convenio Budapest (Convenio Europeo sobre la Ciberdelincuencia 2001): disposiciones específicas
 - Iberoamérica: Tratado de Madrid
- Unión Europea: **Orden Europea de Investigación**



SISTEMA CONVENIO BUDAPEST

- **Convenio sobre la Ciberdelincuencia**, hecho en Budapest el 23-11-2001:
 - A falta de convenio más específico, el Convenio de Budapest puede servir de base para peticiones de asistencia mutua
 - 64 ratificaciones
 - Consejo de Europa: abierto a otros Estados
 - Argentina, Chile, Costa Rica, Panamá, Paraguay, Perú, República Dominicana
 - EEUU, Canadá, Japón, Australia, Marruecos
- **Ámbito de aplicación asistencia mutua (arts. 14 y 25.1):**
 - A los delitos “informáticos” (definidos en el Convenio)
 - Y a la **obtención de pruebas electrónicas de un delito**

SISTEMA DEL CONVENIO BUDAPEST



- **Obtención de datos en tiempo real en Estado requerido**
 - Datos asociados
 - Contenidos

- **Remisión de datos almacenados en el Estado requerido**
 - Conservación
 - Remisión
 - Acceso transfronterizo

OBTENCIÓN EN TIEMPO REAL

- Obtención en tiempo real de **datos asociados al tráfico**:
 - Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en su territorio transmitidas por medio de un sistema informático
 - Se prestará dicha asistencia como mínimo respecto de los delitos por los que se podría conseguir la obtención en tiempo real de datos sobre el tráfico en un caso similar en su país.
- Obtención o grabación en tiempo real de datos sobre el **contenido** de comunicaciones :
 - Cláusula general; y en la medida en que lo permitan sus tratados y el derecho interno aplicables.

CONSERVACIÓN DE DATOS (MEDIDAS PROVISIONALES)

- **Conservación rápida de datos almacenados (“congelación”):**
 - Previa a la solicitud de registro o acceso, confiscación o revelación de los datos
 - Posterior plazo de 60 días para remitir la solicitud (CRI) de los datos
- **Revelación rápida de datos conservados:**
 - Si en la ejecución de una solicitud de conservación rápida de datos, la Parte Requerida descubre que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación: revelará rápidamente a la Parte Requiriente un volumen suficiente de datos para identificar al proveedor de servicios y la vía por la que se transmitió la información

REMISIÓN DE DATOS

- Una Parte podrá solicitar a otra Parte que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un **sistema informático situado en el territorio de la Parte requerida**
- Respuesta: por convenio internacional aplicable; por defecto, con base en Convenio Budapest
- Se dará respuesta lo antes posible si los datos pertinentes están especialmente expuestos al riesgo de pérdida o modificación



ACCESO TRANSFRONTERIZO A DATOS

Una Parte podrá, sin la autorización de otra Parte:

- Tener acceso a datos informáticos almacenados que se encuentren a disposición del público (**fuelle abierta**), con independencia de la ubicación geográfica de dichos datos; o
- Tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra Parte, si la Parte obtiene el **consentimiento** lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático.

IBEROAMÉRICA: TRATADO DE MADRID

“Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia” (Madrid, 28 mayo 2014)

- Ratificado por Nicaragua, Portugal, Perú, Uruguay, Nicaragua, Costa Rica, Cuba, entre otros
- Objeto: reforzar la cooperación mutua de las Partes para la adopción de medidas de aseguramiento y obtención de pruebas para la lucha contra la ciberdelincuencia
 - “ciberdelincuencia”: cualquier forma de criminalidad ejecutada en el ámbito de interacción social definido por el uso de las Tecnologías de la Información y la Comunicación



TRATADO DE MADRID

MEDIDAS DE ASEGURAMIENTO

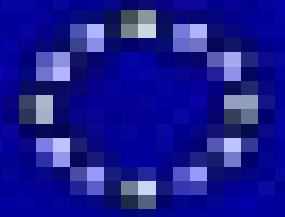
- 1. La incautación y depósito de sistemas informáticos o soportes de almacenamiento de datos.
- 2. El sellado, precinto y prohibición de uso de sistemas informáticos o soportes de almacenamiento de datos.
- 3. El requerimiento de preservación inmediata de datos que se hallan en poder de terceros.
- 4. La copia de datos.

DILIGENCIAS DE INVESTIGACIÓN

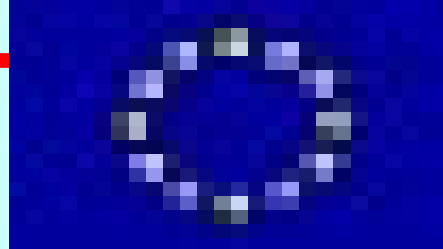
- 1. La intervención de comunicaciones a través de las tecnologías de la información y comunicación.
- 2. La obtención de datos de tráfico.
- 3. El acceso a sistemas de información.
- 4. Acceso a la información contenida en un dispositivo que permita el almacenamiento de datos.
- 5. La entrega de datos y archivos informáticos.

- **TRATADO DE MEDELLÍN transmisión electrónica de solicitudes de cooperación jurídica internacional entre Autoridades Centrales**
 - CRI: remisión y respuesta en formato electrónico a través de la plataforma Iber@
 - Para cualquier CRI, también en materia de investigación y prueba: está incluida la prueba digital
 - Se ha de fundamentar en un instrumento internacional aplicable





- **Orden Europea de Investigación (OEI)**
 - Directiva 2014/41/CE;
 - Transpuesta en España por Ley 23/2014 (reformada por Ley 3/2018)
 - Idea de reconocimiento mutuo de resoluciones judiciales
- **Posibilidades:**
 - Interceptación de comunicaciones: normativa específica
 - Remisión datos (OEI general): para conservación rápida de datos; y para la remisión de los datos
- **Futuro:** Propuesta de Reglamento sobre Órdenes Europeas de Producción y Preservación de Evidencias Electrónicas en materia criminal (llamada E-Evidence)



UNIÓN EUROPEA	VIGENTE	FUTURO
INTERVENCIÓN COMUNICACIONES	Orden Europea de Investigación (específica)	Orden Europea de Investigación (específica)
PRESERVACIÓN DATOS	Orden Europea de Investigación (genérica)	Orden Europea de Preservación de e-evidence (específica)
REMISIÓN DATOS	Orden Europea de Investigación (genérica)	Orden Europea de Entrega de e-evidence (específica)

2.- DATOS CONSERVADOS POR LOS PROVEEDORES DE SERVICIOS



RELEVANCIA PARA LA INVESTIGACIÓN Y PRUEBA



- 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

(FUENTE: INFORME UE IMPACTO REGLAMENTO E-EVIDENCE)

ESTRATEGIA INTERNACIONAL

1. Agotar fuentes abiertas y recursos internos

- Fuentes accesibles al público
- Solicitud remitida directamente al proveedor que se encuentre establecido o registrados en el país; o bien a la filial del Proveedor localizada en nuestro país

2. Solicitud internacional alternativa a la Comisión Rogatoria formal

- Solicitud directa al proveedor de servicios situado en otro país.
- Contacto directo con el usuario de una cuenta para proporcionar datos descargados de dicha cuenta
- Consentimiento del usuario de la cuenta (o sus familiares más cercanos en caso de fallecimiento) para que el proveedor proporcione datos de la citada cuenta
- Cooperación policial, ya sea mediante procedimiento legalmente establecido, o bien mediante entrega voluntaria

3. Uso de la Asistencia Judicial Internacional

- Acudir a 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, por lo que seguidamente se recogen una serie de **recomendaciones** para mejorar la eficacia de la solicitud

DECÁLOGO DE RECOMENDACIONES

1. Incluir una **descripción precisa de los datos** solicitados. Para los aspectos técnicos de la solicitud, resulta conveniente realizar una consulta previa a la unidad policial especializada.
2. Claridad y sencillez en la **descripción de los hechos**, especialmente para facilitar la traducción. Y asegurar una buena **calidad de la traducción** de su solicitud.
3. Incluir una referencia a los motivos que justifiquen la **necesidad y utilidad** de los datos requeridos para la concreta investigación penal (juicio de pertinencia); así como a la razón para que se practique en este momento (**actualidad**)
4. Asegurarse de la **gravedad del delito** e incluir en la solicitud información relativa a la misma. Esta gravedad se puede concretar en el **perjuicio económico causado** por el delito (téngase en cuenta que en EEUU exigen un mínimo de 5.000 dólares por daños y perjuicios); o bien en **otros elementos** ligadas a las circunstancias de la víctima, a las características del delito y/o a la existencia de una estructura criminal. Cabe señalar que EEUU no suele ejecutar solicitudes en relación con delitos relativos a la libertad de expresión o con delitos de odio.
5. Los requisitos de fundamentación de la solicitud serán más elevados cuanto **mayor sea la afectación de los derechos fundamentales** en los datos solicitados. Por ejemplo, si desea obtener el contenido de un correo electrónico, generalmente se tendrá que proporcionar más evidencia de la que se tendría que suministrar para obtener una mera información sobre el abonado; en Estados Unidos se exige en estos casos la existencia de “causa probable”.

DECÁLOGO DE RECOMENDACIONES (2)

6. Señalar si concurre **urgencia**, resultando aconsejable explicar los motivos que la justifiquen
7. Mantener contacto durante su ejecución, haciendo el correspondiente **seguimiento**, sobre todo para conocer y remover las causas de un posible retraso. Y proporcionar los datos de las **personas de contacto**, tanto para la comunicación oficial como para la informal.
8. Indicar el **régimen de confidencialidad** deseado.
9. Solicitar un **acuse de recibo** de su solicitud.
10. Analizar la posibilidad de remitir una **solicitud de preservación o “congelación de datos”** (antes de la petición de remisión del dato por CRI) para evitar el borrado de los datos que se necesitan. Téngase en cuenta que existen **determinados tipos de datos que se borran con rapidez** por los proveedores (por ejemplo, logs o registros de transmisión, información del suscriptor, contenido del correo electrónico e informaciones de sitios web), lo que deviene especialmente relevante en aquellos **Estados que no contienen una obligación legal general de retención de datos** para las investigaciones penales (entre los que destacan Estados Unidos y determinados países europeos). Hay que tener en cuenta que, una vez eliminados, los datos generalmente no se pueden recuperar por el proveedor.

PROVEEDORES DE SERVICIOS SITUADOS EN ESTADOS UNIDOS



- Acceso a los datos en poder de las operadora: la **mayoría de los servidores de las Redes Sociales (Facebook, Twitter) tienen sus servidores en EEUU.**
- Posibilidades:
 - Solicitud directa al proveedor de servicios: a la sucursal o filial en el país; en otro caso, a la matriz o central en EEUU
 - En otro caso: Comisión Rogatoria Internacional (Acuerdo de asistencia judicial entre los EEUU y la UE firmado el 25 de junio de 2003);
 - En caso de urgencia, determinadas empresas contemplan las llamadas “Emergency Disclosing Requests”,
 - Estas operadoras tienen una política de condiciones, que en la práctica es la que resulta aplicable
- **Guía Práctica Embajada España en EEUU**
 - www.mjusticia.gob.es
- **Futuro: en el marco del Cloud Act**
 - "Ley de clarificación del uso legítimo de los datos fuera de los Estados unidos" (Clarifying Lawful Overseas Use of Data Act o CLOUD Act)
 - las autoridades de aquellos Estados que firmen un acuerdo con EEUU podrán dirigirse a los proveedores en EEUU en las mismas condiciones que si fueran autoridades de EEUU, siempre que se trate de datos sobre nacionales propios o sobre nacionales de otros países que se encuentren en el territorio del Estado requirente. Ya existe un acuerdo con el Reino Unido de octubre de 2019



ÚLTIMAS NOVEDADES

1. Segundo Protocolo del Convenio de Budapest sobre la cibercriminalidad
2. Órdenes Europeas de Producción y Preservación de Evidencias Electrónicas en materia criminal en la UE (llamada E-Evidence)
3. Tratado de la ONU sobre la ciberdelincuencia

SISTEMA CONVENIO BUDAPEST

- **Segundo Protocolo del Convenio sobre la Ciberdelincuencia**
 - Entrada en vigor con 5 ratificaciones (actualmente 2, Serbia y Japón)
- Tres partes:
 1. Medidas de cooperación reforzada en relación con datos informáticos almacenados en otro Estado
 2. Regula con carácter general la asistencia judicial urgente
 3. Videoconferencia; y equipos conjuntos de investigación e investigaciones comunes

2º PROTOCOLO CONVENIO BUDAPEST

PARTE 1ª: medidas de cooperación reforzada en relación con datos informáticos almacenados en otro Estado

- 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
 - Obligación de adoptar medidas 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); y
 - Para la entrega acelerada de **datos informáticos almacenados específicos en caso de urgencia** (artículo 9; Red 24/7; formato electrónico...

Reglamento sobre Órdenes Europeas de Producción y Preservación de Evidencias Electrónicas en materia criminal (llamada E-Evidence)

- **Comunicación directa** entre la autoridad judicial y el proveedor de servicios para solicitar la entrega de datos almacenados
 - Régimen jurídico diferente para cada tipo de datos
- Cada proveedor:
 - Debe designar **representante** a tal fin (Directiva)



CONVENIO ONU CONTRA LA CIBERDELINCUENCIA

- Adoptado por la Asamblea General ONU de 26 de diciembre de 2024
- Se abre a la firma durante 2025
- Entrará en vigor con la firma de 40 Estados

