Cooperación Española
CONOCIMIENTO / INTERCOONECTA

Curso de Especialización Judicial

Ciberdelincuencia: tratamiento preventivo, procesal y sustantivo desde una perspectiva internacional. 4ª Edición

Autor,
Alberto Varona Jiménez
Cargo **Magistrado**
Institución **CGPJ**
País **ESPAÑA**

Consejo General del Poder Judicial
Escuela Judicial

Aula Iberoamericana
Consejo General del Poder Judicial

Consejo General del Poder Judicial
Escuela Judicial

Aula Iberoamericana
Consejo General del Poder Judicial

Cooperación Española
CONOCIMIENTO / INTERCOONECTA

LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA

Alberto Varona Jiménez
Magistrado

Marzo 2025

- **Dificultades técnicas:** metodología criminalística. Dominio de la informática y normas del proceso.

- **La volatilidad de las huellas digitales:** memoria RAM y en tránsito

- **Carácter transnacional:** el ciberespacio
- **Afectación de derechos fundamentales**

FASES

- ~~Obtención de las evidencias: digitales y electrónicas~~
- Aseguramiento de las evidencias
- Acto pericial
- Emisión del informe pericial
- Practica de la prueba pericial
- Valoración en la sentencia

- PRIMER TRATADO INTERNACIONAL DE DELITOS INFORMÁTICOS
- **ARMONIZAR** leyes nacionales.
- **MEJORAR** técnicas de investigación.
- AUMENTAR la cooperación entre naciones.
- CUESTIONES DE DERECHO PROCESAL

MEDIDAS

- **Título 2. Conservación rápida de datos informáticos almacenados**
  - Conservación rápida de datos informáticos almacenados (art. 16)
  - Conservación y revelación parcial rápidas de datos de tráfico (art. 17)
- **Título 3**. **Orden de presentación** (art. 18)
- **Título 4. Registro y confiscación** de datos informáticos almacenados (art. 19)
- **Título 5**. **Obtención en tiempo real de datos informáticos**
  - Obtención en tiempo real de datos sobre el tráfico (art. 20)
  - Interceptación de datos sobre el contenido (art. 21)

ESQUEMA

- **DATOS INFORMÁTICOS ALMACENADOS**
  - Conservación rápida (art. 16)
  - Revelación parcial (art. 17)
  - Orden de presentación (art. 18)
  - Registro y confiscación (art. 19)

- **DATOS INFORMÁTICOS EN TIEMPO REAL**
  - **DATOS SOBRE EL TRÁFICO:** Obtención (art. 20)
  - **DATOS SOBRE EL CONTENIDO:** Interceptación (art. 21)

DATOS INFORMÁTICOS

Cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función.

PRINCIPIO DE LEGALIDAD (art. 14.1 y 2)

INVESTIGACIONES O PROCEDIMIENTOS PENALES
ESPECÍFICOS

TIPOS DELICTIVOS

a) Los delitos previstos de conformidad con los artículos 2 a 11 del presente Convenio;

b) otros delitos cometidos por medio de un sistema informático; y

c) la obtención de pruebas electrónicas de un delito.

PRINCIPIOS RECTORES (art. 15)

1. Cada Parte se asegurará de que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deberá garantizar una **protección adecuada de los derechos humanos** y de las libertades, incluidos los derechos derivados de las obligaciones asumidas en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950), del Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966), y de otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando resulte procedente dada la naturaleza del procedimiento o del poder de que se trate, dichas condiciones incluirán, entre otros aspectos, la **supervisión judicial u otra forma de supervisión independiente**, **los motivos que justifiquen la aplicación, y la limitación del ámbito de aplicación y de la duración del poder o del procedimiento de que se trate.**

3. Siempre que sea conforme con el interés público y, en particular, con la correcta administración de la justicia, cada Parte examinará la repercusión de los poderes y procedimientos previstos en la presente sección en los derechos, responsabilidades e **intereses legítimos de terceros.**

CONTENIDO DE LA RESOLUCIÓN JUDICIAL EN ESPAÑA (art. 588 bis c.3)

a) El **hecho punible** objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.

b) La **identidad** de los investigados y de cualquier otro afectado por la medida, de ser conocido.

c) La **extensión** de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los **principios rectores** establecidos en el artículo 588 bis a.

d) La **unidad investigadora** de Policía Judicial que se hará cargo de la intervención.

e) **La duración** de la medida.

f) La **forma y la periodicidad** con la que el solicitante informará al juez sobre los resultados de la medida.

g) La **finalidad perseguida** con la medida.

h) El **sujeto obligado** que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

CONSERVACIÓN RÁPIDA DE DATOS INFORMÁTICOS ALMACENADOS (ART. 16)

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera

la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación.

ESQUEMA

- **DATOS INFORMÁTICOS ALMACENADOS**
  - Conservación rápida (art. 16)
  - Revelación parcial (art. 17)
  - Orden de presentación (art. 18)
  - Registro y confiscación (art. 19)

- **DATOS INFORMÁTICOS EN TIEMPO REAL**
  - **DATOS SOBRE EL TRÁFICO:** Obtención (art. 20)
  - **DATOS SOBRE EL CONTENIDO:** Interceptación (art. 21)

CONSERVACIÓN Y REVELACIÓN RÁPIDAS DE DATOS SOBRE EL TRÁFICO ALMACENADOS (ART. 17)

PARA GARANTIZAR LA CONSERVACIÓN DE LOS DATOS SOBRE EL TRÁFICO en aplicación de lo dispuesto en el artículo 16 (…)

Por «datos sobre el tráfico» se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

CONSERVACIÓN Y REVELACIÓN RÁPIDAS DE DATOS SOBRE EL TRÁFICO ALMACENADOS (ART. 17)

PARA GARANTIZAR LA CONSERVACIÓN DE LOS DATOS SOBRE EL TRÁFICO en aplicación de lo dispuesto en el artículo 16,

cada Parte adoptará las **medidas legislativas y de otro tipo que resulten necesarias**:

a) Para asegurar la posibilidad de conservar rápidamente dichos datos sobre el tráfico **con independencia** de que en la transmisión de esa comunicación **participaran uno o varios proveedores de servicios**, y

b) para garantizar la **revelación rápida** a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos sobre el tráfico para que dicha Parte pueda identificar a los proveedores de servicio y la vía por la que se transmitió la comunicación.

EN ESPAÑA (art. 588 octies) Orden de conservación de datos

- **Artículo 588 octies. Orden de conservación de datos.**
- El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes.
- Los datos se conservarán durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días.
- El requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, quedando sujeto a la responsabilidad descrita en el apartado·3 del artículo 588 ter e.

ESQUEMA

- **DATOS INFORMÁTICOS ALMACENADOS**
  - Conservación rápida (art. 16)
  - Revelación parcial (art. 17)
  - Orden de presentación (art. 18)
  - Registro y confiscación (art. 19)

- **DATOS INFORMÁTICOS EN TIEMPO REAL**
  - **DATOS SOBRE EL TRÁFICO:** Obtención (art. 20)
  - **DATOS SOBRE EL CONTENIDO:** Interceptación (art. 21)

ORDEN DE PRESENTACIÓN (art. 18)

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a) A **una persona** que se encuentre en su territorio que comunique determinados **datos informáticos** que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y

b) a **un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte** que comunique los **datos** que posea o que se encuentren bajo su control relativos a los **abonados** en conexión con dichos servicios.

DATOS RELATIVOS A LOS ABONADOS (art. 18.3)

3. A los efectos del presente artículo, por «**datos relativos a los abonados**» se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:

a) El tipo de servicio de comunicaciones utilizado, las **disposiciones técnicas** adoptadas al respecto y el periodo de servicio;

b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;

c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

ESQUEMA

- **DATOS INFORMÁTICOS ALMACENADOS**
  - Conservación rápida (art. 16)
  - Revelación parcial (art. 17)
  - Orden de presentación (art. 18)
  - Registro y confiscación (art. 19)

- **DATOS INFORMÁTICOS EN TIEMPO REAL**
  - **DATOS SOBRE EL TRÁFICO:** Obtención (art. 20)
  - **DATOS SOBRE EL CONTENIDO:** Interceptación (art. 21)

REGISTRO Y CONFISCACIÓN (art. 19)

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes **a registrar** o a tener acceso de una forma similar:

a) A un **sistema informático o a una parte** del mismo, así como a los **datos informáticos** almacenados en el mismo; y

b) a un **medio de almacenamiento** de datos informáticos en el que puedan almacenarse datos informáticos, en su territorio.

LA NUBE (art. 19.2)

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo, de conformidad con lo dispuesto en el apartado 1.a, y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado **en su territorio**, y dichos datos sean **lícitamente accesibles a través del sistema inicial o estén disponibles para éste**, dichas autoridades puedan ampliar rápidamente el registro o la forma de acceso similar al otro sistema.

EN ESPAÑA (art. 588 sexies c. 3)

Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. En caso de urgencia, la Policía Judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación

CONFISCAR (art. 19.3)

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de una forma similar los datos informáticos a los que se haya tenido acceso en aplicación de lo dispuesto en los apartados 1 ó 2. Estas medidas incluirán las siguientes facultades:

a) **Confiscar** u obtener de una forma similar un sistema informático o una parte del mismo, o un medio de almacenamiento de datos informáticos;

b) Realizar y conservar una **copia** de dichos datos informáticos;

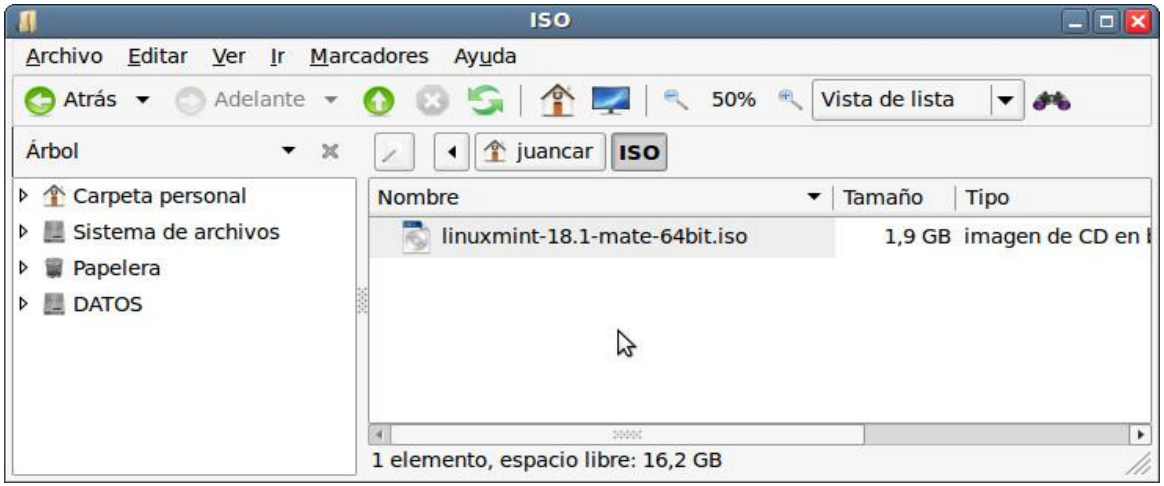
c) **Preservar** la integridad de los datos informáticos almacenados de que se trate;

d) **Hacer inaccesibles** o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso.

CLONACIÓN

¿CÓMO SE REALIZA: HARDWARE/~~SOFTWARE~~

- IMAGEN FORENSE
- FIRMA DIGITAL



DEBER DE COLABORACIÓN (art. 19.4)

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a **ordenar a cualquier persona que conozca el funcionamiento** del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que **facilite toda la información necesaria**, dentro de lo razonable, para permitir la aplicación de las medidas indicadas en los apartados 1 y 2.

ESQUEMA

- **DATOS INFORMÁTICOS ALMACENADOS**
  - Conservación rápida (art. 16)
  - Revelación parcial (art. 17)
  - Orden de presentación (art. 18)
  - Registro y confiscación (art. 19)

- **DATOS INFORMÁTICOS EN TIEMPO REAL**
  - **DATOS SOBRE EL TRÁFICO:** Obtención (art. 20)
  - **DATOS SOBRE EL CONTENIDO:** Interceptación (art. 21)

DATOS INFORMÁTICOS EN TIEMPO REAL (arts. 20 y 21)

ART. 20 **DATOS SOBRE EL TRÁFICO**:

OBTENCIÓN en tiempo real los datos sobre el tráfico asociados a comunicaciones específicas **transmitidas en su territorio** por medio de un **sistema informático. POSIBILIDAD DE RESERVA**

ART. 21 **DATOS SOBRE EL CONTENIDO:**

INTERCEPTACIÓN en tiempo real los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático, respecto a una serie de **delitos graves** que deberán definirse en el derecho interno

CONCEPTO DE OBTENCIÓN O INTERCEPTACIÓN

a) A **obtener o a grabar** mediante la aplicación de medios técnicos existentes en su territorio, y

b) a **obligar** a un **proveedor de servicios**, dentro de los límites de su capacidad técnica: i) A **obtener o a grabar** mediante la aplicación de los medios técnicos existentes en su territorio, o ii) a **prestar** a las autoridades competentes su colaboración y su asistencia para obtener o grabar

DEBER DE SECRETO (arts. 20.3 y 21.3)

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS:

1.ºDelitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.

2.º Delitos cometidos en el seno de un grupo u organización criminal.

3.º Delitos de terrorismo.

4.º Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación

COMUNICACIONES ORALES:

1.ºDelitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.

2.º Delitos cometidos en el seno de un grupo u organización criminal.

3.º Delitos de terrorismo.

REGISTROS REMOTOS

a) Delitos cometidos en el seno de organizaciones criminales.

b) Delitos de terrorismo.

c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.

d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.

e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

ESQUEMA

- **DATOS INFORMÁTICOS ALMACENADOS**
  - Conservación rápida (art. 16)
  - Revelación parcial (art. 17)
  - Orden de presentación (art. 18)
  - Registro y confiscación (art. 19)

- **DATOS INFORMÁTICOS EN TIEMPO REAL**
  - **DATOS SOBRE EL TRÁFICO:** Obtención (art. 20)
  - **DATOS SOBRE EL CONTENIDO:** Interceptación (art. 21)

Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia, hecho en Madrid el 28 de mayo de 2014

CONVENIO IBEROAMERICANO DE COOPERACIÓN SOBRE INVESTIGACIÓN, ASEGURAMIENTO Y OBTENCIÓN DE PRUEBA EN MATERIA DE CIBERDELINCUENCIA

Última actualización 19/10/2023

Partes	Estados firmantes de la COMJIB y otros Estados que se adhieran.
Entrada en vigor y vigencia	En vigor a partir del 26 de agosto 2022. Después del depósito de tres instrumentos de ratificación. Vigencia: indefinida
Firma	Firmado en Madrid, 28 mayo 2014 por representantes de: Guatemala, Portugal, Nicaragua, Uruguay y Perú. Los Estados Unidos Mexicanos firmaron ad referéndum el 9 de junio de 2014 con intención de adherirse. Costa Rica firmó ad referéndum el 12 junio 2014 con intención de adherirse.
Depósito Ratificación o Adhesión	Cuba: depositó el instrumento de adhesión 18 de julio 2016. Nicaragua: ratificado por Decreto Presidencial N°. 08-2020, aprobado el 16 de Abril de 2020, el deposito del instrumento 27 de julio de 2022. Uruguay: depositó el instrumento de ratificación 26 de enero 2022. Posterior a la firma del 28 de mayo de 2014 para los Estados que quieran ser parte sólo procede la adhesión.
Pendientes de ratificación	México, Costa Rica, Guatemala, Portugal y Perú. El resto de los miembros de la COMJIB podría adherirse.

COMJIB

OBJETO (art. 1)

El presente convenio tiene por objeto reforzar la cooperación mutua de las Partes para la adopción de medidas de aseguramiento y obtención de pruebas para la lucha de la ciberdelincuencia

Artículos 6 y 2: MEDIDAS DE ASEGURAMIENTO

- La incautación y depósito de sistemas informáticos o soportes de almacenamiento:

  "Ocupación física y su aseguramiento por las autoridades"

- El **sellado, precinto** y prohibición de uso de sistemas informáticos o soportes de almacenamiento:

  "Bloqueo absoluto o imposibilidad de su utilización, incluida la congelación de sistemas virtuales"

- El requerimiento de preservación inmediata de datos que se hallan en poder de terceros:

  "Deber de conservación íntegra de la información digital que obre en su poder o sobre la que tenga facultades de disposición".

- La copia de datos

  "Reproducción exacta de la información digital recolectada por particulares o entidades publicas o privadas"

Artículo 7: MEDIDAS DE OBTENCIÓN DE EVIDENCIAS

- Intervención de las comunicaciones
- Obtención de datos de tráfico
- Acceso a sistemas de información
- Acceso a la información contenida en un dispositivo de almacenamiento de datos
- Entrega de datos y archivos informáticos

Consejo General del Poder Judicial
Escuela Judicial

Aula Iberoamericana
Consejo General del Poder Judicial

Cooperación Española
CONOCIMIENTO / INTERCOONECTA

MUCHAS GRACIAS POR SU ATENCIÓN

ALBERTO VARONA JIMÉNEZ
a.varona@poderjudicial.es