Ciberdelitos: el nuevo desafío del Derecho en la era digital

Palencia, 4 de noviembre de 2025

Ilustre Colegio Provincial de
Abogados de Palencia

Ciberdelito

Ciberdelito

En el vigente Código Penal no se halla un título específico que contenga los delitos que coloquialmente conocemos como "informáticos". En su articulado, se encuentran diseminados multitud de tipos penales cuya comisión cabría dentro del concepto amplio de "delito informático".

Podríamos definir delito informático o ciberdelito a todo ilícito penal llevado a cabo a través de medios telemáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

Tipoligía delictiva

Convenio sobre ciberdelincuencia Budapest NOV´01

Título 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

HACKING

Título 2. Delitos informáticos

FRAUDES

Título 4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

PROPIEDAD INTELECTUAL

Título 3. Delitos relacionados con el contenido

PORNOGRAFÍA INFANTIL

Marco legislativo: Código Penal

- **Amenazas** (artículo 169 y 171)
- **Coacciones** (art. 172)
- **Hostigamiento** (***stalking*** art. 172 ter.)
- **Contra la integridad moral** (art. 173.1) (***acoso escolar, bullying y ciberbullying***).
- **Abusos sexuales** (Artículo 181.1 y 2).
- **Abusos y Agresiones Sexuales a Menores de 16 años** (art. 183, 183 bis) (***grooming*** art. 183 ter)
- **Acoso sexual** (art. 184)
- **Exhibicionismo y provocación sexual** (artículos 185 y 186).
- **Delitos relativos a la prostitución y la corrupción de menores** (artículos 187 y 189).
- **Descubrimiento y revelación de secretos** (artículos 197 a 201) (***sexting*** art. 197.7 bis).
- **Calumnias** (artículos 205, 206 y 207).
- **Injurias** (artículos 208, 209 y 210).
- **Estafas** (artículos 249 y 250).
- **Defraudaciones de fluido eléctrico y análogas** (artículos 255 y 256).
- **Daños** (artículos 263 a 267) (***informáticos*** art. 264) (***ataques informáticos*** art. 264 bis)
- **Delitos relativos a la propiedad intelectual** (art. 270).
- **Delitos relativos a la propiedad industrial** (artículos 273 y 274).

Marco legislativo: Código Penal

- **Delitos relativos al mercado y a los consumidores** (***descubrimiento de secreto de empresa*** Arts. 278 a 280 y 285), (***acceso a servicios de radiodifusión o interactivos*** art. 286).
- **Delitos contra la salud pública** (artículos 359 a 363)
- **Falsedades** (artículos 386.1, 388, 390, 392, 395, 399.1 bis y 400)
- **Usurpación del estado civil** (art. 401)
- **Delitos cometidos con ocasión del Ejercicio de los Derechos Fundamentales y de las Libertades Públicas garantizados por la Constitución** (***apología del racismo y xenofobia, negación o justificación de los delitos de genocidio*** art. 510)
- **Delitos Contra el Orden Público** (***incitación*** art. 559)
- **Tenencia, tráfico y depósito de armas, municiones o explosivos** (***comercialización*** art. 566)
- **Delitos de terrorismo** (***adoctrinamiento o adiestramiento*** art. 575), (***colaboración con organización, grupo o elemento terrorista*** art. 577.1), (***enaltecimiento o justificación del terrorismo*** art. 578.2)
- **Cualquier otro delito que sea punible por "*provocación, conspiración o proposición*", cometido a través o mediante tecnologías de la información y las comunicaciones.**

Marco legislativo

INSTRUCCIÓN 2/2011
SOBRE EL FISCAL DE SALA DE CRIMINALIDAD INFORMÁTICA Y LAS SECCIONES DE CRIMINALIDAD INFORMÁTICA DE LAS FISCALÍAS

Instrucción FGE 2/2011

1) Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs.

-Delitos de **daños, sabotaje informático y ataques de denegación de servicios previstos** y penados en el artículo 264 y concordantes del Código Penal.

-Delitos de **acceso sin autorización a datos, programas o sistemas informáticos** previstos y penados en el artículo 197.2 del Código Penal.

-Delitos de **descubrimiento y revelación de secretos** del artículo 197 del Código Penal cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos.

-Delitos de **descubrimiento y revelación de secretos de empresa previstos** y penados en el artículo 278 del Código Penal cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos ó electrónicos.

-Delitos **contra los servicios de radiodifusión e interactivos** previstos y penados en el artículo 286 del Código Penal.

Instrucción FGE 2/2011

2) Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs.

-Delitos de **estafa** previstos y penados en el artículo 248.2 a) b) y c) del Código Penal, siempre que, en los supuestos a) y c) **se utilicen las TICs** para llevar a efecto la transferencia u operación de cualquier tipo en perjuicio de otro.

-Delitos de **acoso a menores de 13 años, child grooming**, previstos y penados en el art. 183 bis del Código Penal cuando se lleve a efecto a través de las **TICs**.

-Delitos de **corrupción de menores o de personas discapacitadas o relativas a pornografía infantil o referida a personas discapacitadas** previstos y penados en el artículo 189 del Código Penal cuando para el desarrollo y/o ejecución de la actividad delictiva se utilicen las TICs.

-Delitos **contra la propiedad intelectual** de los artículos 270 y ss del Código Penal cuando se cometan utilizando las TICs.

Instrucción FGE 2/2011

C) Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia.

-Delitos de **falsificación documental** de los artículos 390 y ss del Código Penal. Para la ejecución del delito se hubieran empleado las **TICs** , determinante en la actividad delictiva de especial complejidad en la investigación.

-Delitos de **injurias y calumnias** contra funcionario público, autoridad o agente de la misma previstos y penados en los artículos 211 y ss del Código Penal cometidos a través de las **TICs**. Circunstancia fuera determinante en la actividad delictiva y complejidad en la inv. crim.

-Delitos de **amenazas y coacciones** previstos y penados en los artículos 169 y ss del Código Penal cometidos a través de las **TICs** . Circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Delitos **contra la integridad moral** previstos y penados en el artículo 173.1 del Código Penal cometidos a través de las **TICs** siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Delitos de **apología o incitación a la discriminación, el odio y la violencia o de negación o justificación de los delitos de genocidio** previstos y penados en los artículos 510 y 607.2 del Código Penal cometidos a través de las **TICs.** Circunstancia fuera determinante en la actividad delictiva y complejidad en la inv. crim.

-**Cualquier otro tipo delictivo en cuya ejecución haya sido determinante la utilización de las TICs** y en los que dicha circunstancia genere una especial complejidad en la investigación criminal.

Ley Orgánica 13/2015.

De 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

CAPÍTULO IV

Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos

Ley Orgánica 13/2015 (art. 588).

Disposiciones comunes. Principios rectores (art. 588.bis.).

Determinación de los principios rectores que han de regir las diligencias de investigación que requieran intromisión en derechos y libertades fundamentales:

- **Proporcionalidad**
- **Especialidad**
- **Idoneidad**
- **Necesidad**
- **Excepcionalidad**

Entre otros criterios para la ponderación de la proporcionalidad se establece el **ámbito tecnológico de producción del delito**

Determinación del alcance y contenido de la medida

- En la solicitud por el Mº Fiscal o Policía Judicial (588 bis b)
- En la resolución judicial (588 bis c)

Ley Orgánica 13/2015 (art. 588).

Intervención e interceptación legal de las comunicaciones telefónicas y telemáticas (art. 588 ter)

Determinación de los delitos que permiten la adopción de estas medidas.

Art. 588 ter. a).- Presupuestos

- **Delitos previsto en el art. 579.1**
  - **Delitos dolosos castigados con pena con límite max. de al menos tres años de prisión.**
  - **Delitos cometidos en el seno de grupo u organización criminal.**
  - **Delitos de terrorismo.**

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

Ley Orgánica 13/2015 (art. 588).

Intervención e interceptación legal de las comunicaciones telefónicas y telemáticas (art. 588. ter.)

- ✓ Proporciona un **concepto legal de datos electrónicos de tráfico o asociados** (588 ter b)
- ✓ Establece el **deber de colaboración** de los operadores de comunicaciones, **prestadores de servicio** de la SI y de toda persona que facilite comunicaciones. Deber de sigilo sobre las actuaciones para las que son requeridos por la autoridad judicial (588 ter e).
- ✓ Determina el **periodo de duración de las intervenciones**: tres meses prorrogables hasta un máximo de 18 meses (588 ter g)
- ✓ Regula detalladamente el **acceso de las partes a las grabaciones** (588 ter i) **y transcripciones realizadas** (588 ter, i)

Ley Orgánica 13/2015 (art. 588).

Incorporación al proceso de datos almacenados (art. 588. ter j.)

- **Sujetos obligados:**
  –Prestadores de servicio:
  – Cualquier persona física o jurídica que facilite la comunicación
- **Deber de colaboración: 588 ter e)**
  Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones
- **Objeto: los datos de tráfico o asociados**
  - Conservados en cumplimiento de la LCD
  - Almacenados por propia iniciativa
- **Solicitud judicial**
  –Datos vinculados a un proceso de comunicación

Ley Orgánica 13/2015 (art. 588).

Acceso a los datos necesarios para la identificación de los usuarios, terminales y dispositivos de conectividad (art. 588. ter k.)

- **Identificación de IP de origen**
  No se requerirá autorización judicial si puede ser localizada en internet por cualquier internauta

- **Resolución de IP**
  Se establece la forma y garantías para la identificación y localización del equipo o dispositivo de conexión e identificación de usuario a partir de la dirección IP utilizada para la comisión del delito.

Solicitud al juez para que requiera la cesión de los datos que permitan la determinación y localización del terminal o del dispositivo de conectividad y la identificación personal del usuario a que fue asignada a los agentes sujetos al deber de colaboración

Ley Orgánica 13/2015 (art. 588).

Acceso a los datos necesarios para la identificación de los usuarios, terminales y dispositivos de conectividad (art. 588. ter l.)

- **Identificación de terminales mediante captación de códigos de identificación del dispositivo o de sus componentes.**

- La Policía Judicial podrá utilizar artificios técnicos para la identificación de aparatos de telecomunicación cuando no haya podido obtener el número de abonado y este sea necesario para la investigación
- A partir de los datos obtenidos habrá de efectuarse solicitud de autorización judicial de intervención.
- Deberá ponerse en conocimiento del órgano judicial la utilización de dichos artificios.

Ley Orgánica 13/2015 (art. 588).

Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad (art. 588. ter, m)

Cesión de datos desvinculados de los procesos de comunicación concernientes a la titularidad o identificación de un dispositivo electrónico

- El Fiscal o la Policía Judicial, **sin necesidad de autorización judicial**, pueden dirigirse directamente a los prestadores de servicio de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información para la obtención de la identidad del titular de un número de teléfono o de otro medio de comunicación o, a la inversa, el número de teléfono o datos de identificación de cualquier otro medio de comunicación (588 ter m).

- Los prestadores estarán obligados a cumplir el requerimiento

Ley Orgánica 13/2015 (art. 588).

Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (art. 588. quater)

- **Grabación de las comunicaciones orales directas. Captación de imágenes en lugares o espacios públicos, domicilio privado o lugar cerrado. (Art. 588 quater a.).**

1. Podrá autorizarse la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados.
2. Los dispositivos de escucha y grabación podrán ser colocados tanto en el exterior como en el interior del domicilio o lugar cerrado.
3. En el supuesto en que fuera necesaria la entrada en el domicilio o en alguno de los espacios destinados al ejercicio de la privacidad, la resolución habilitante habrá de extender su motivación a la procedencia del acceso a dichos lugares.
4. Presupuestos (art. 588 quater b).
5. Contenido de la resolución judicial (art. 588 quater c)
6. Control de la media (art. 588 quater d).
7. Cese (art. 588 quater e).

Ley Orgánica 13/2015 (art. 588).

Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (art. 588. quinquies)

- ***Captación de imágenes en lugares o espacios públicos.*** ***(art. 588 quinquies a.).***
- ***Utilización de dispositivos o medios técnicos de seguimiento y localización.*** ***(art* 588 quinquies b.)**
  1. Acreditadas razones de necesidad y la medida resulte proporcionada, el juez competente podrá autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización.
  2. La autorización deberá especificar el medio técnico a utilizar.
  3. Deber de colaboración de prestadores de servicios (art. 588, ter e),
  4. Cuando concurran razones de urgencia (temor no colocación dispositivo), la Policía Judicial podrá proceder a su colocación, dando cuenta a la mayor brevedad posibl,. O en el plazo máximo de veinticuatro horas, a la autoridad judicial, quien ratificará la medida o acordará su cese inmediato (la información obtenida a partir del dispositivo colocado carecerá de efectos en el proceso).
  5. Duración máxima medida 3 meses. Excepcionalmente prórrogas hasta máximo de 18 meses.

Ley Orgánica 13/2015 (art. 588).

Registro de sistemas informáticos y dispositivos de almacenamiento masivo (art. 588. sexies)

- **Con ocasión de Registro domiciliario -588 sexies a)**
  - Cuando sea previsible la aprehensión de tales instrumentos
  - Requiere **motivación individualizada** en la Autorización judicial
- **Fuera del domicilio del investigado- 588 sexies b)**
  - Con iguales exigencias.
- **La autorización judicial -588 sexies c) :**
  - Determinará los **términos y alcance del registro y las condiciones que aseguren la integridad** de datos y garantías de su preservación .
  - Principio general de no incautación de dispositivos físicos cuando perjudique a su titular y se puedan obtener copias en condiciones de autenticidad e integridad
  - **Posibilidad de ampliación a otros sistemas lícitamente accesibles desde el sistema inicial** .
  - **Casos de urgencia: concurra interés constitucional cabrá el examen directo sin Autorización.** Y posterior comunicación inmediata y motivada al Juez en máximo de 4 horas

Ley Orgánica 13/2015 (art. 588).

Registro remotos sobre equipos informáticos (art. 588 septies)

- ***Utilización de datos de identificación y códigos, la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos. (art. 588 septies a). Delitos:***
  a) Cometidos en el seno de organizaciones criminales.
  b) Terrorismo.
  c) Cometidos contra menores o capacidad modificada judicialmente.
  d) Contra la Constitución, de traición y relativos a la defensa nacional.
  e) Cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.
- ***Resolución judicial.***
- ***Deber de colaboración.***
- ***Duración.-*** Máx. 1 mes prorrogable hasta máximo de 3 meses.

Ley Orgánica 13/2015 (art. 588).

Registro remoto de forma telemática de ordenadores y sistemas informáticos (art. 588 septies)

- **Dos técnicas de investigación**
  - Uso de datos de identificación y códigos
  - Instalación de software
- **Solo para supuestos excepcionales:**
  - Medida imprescindible
  - Solo en para los supuestos legalmente establecidos
    - Delitos muy graves: terrorismo, en el seno de organizaciones criminales, contra menores o personas con capacidad modificada judicialmente, contra la Constitución, traición y relativos a la defensa nacional.
    - **Delitos cometidos a través de instrumentos informáticos o cualquier otra tecnología de la comunicación o la telecomunicación o servicio de comunicación**
- **Determinación en la autorización,** alcance y contenido**,** software, mediante el cual se ejecutará el control de la información, las medidas precisas para preservación de la integridad de los datos, su inaccesibilidad o supresión del sistema informático donde se encuentran

Ley Orgánica 13/2015 (art. 588).

Nuevas técnicas de investigación.

Agente encubierto informático (art. 282 bis, 6 y 7)

Extensión de la figura del agente encubierto: adaptación a las exigencias de la investigaciones on line.-

- El juez podrá autorizar a la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación para esclarecer los delitos previstos en el 282 bis. 4 y **cualquier delito cometido a través de las tecnologías de la información y la comunicación** (282 bis por remisión al 588 ter a.)
- Con autorización específica para ello, el agente encubierto podrá **enviar o intercambiar por si mismo archivos ilícitos** por razón de su contenido y analizar el resultado de los algoritmos aplicados para la identificación de dichos archivos
- Lo previsto en el artículo 282 bis. 7 puede ser de aplicación a la actividad del agente encubierto on-line cuando en el curso de comunicaciones telemáticas entre el agente y el investigado se estima necesaria la **captación de imágenes o grabación de conversaciones**. Precisa específica autorización judicial.

Circulares FGE

- **Circular 1/2019**, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal

- **Circular 2/2019**, sobre interceptación de comunicaciones telefónicas y telemáticas

- **Circular 3/2019**, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos

- **Circular 4/2019**, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización

- **Circular 5/2019**, sobre registro de dispositivos y equipos informáticos

Ley Orgánica 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso

Dos. Se modifica la redacción del artículo 248, que queda redactado como sigue:

«Artículo 248.

Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre este y el defraudador, los medios empleados por este y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.

Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses.»

Ley Orgánica 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso

Tres. Se modifica el artículo 249, que queda redactado como sigue:

«Artículo 249.

1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años:

a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

2. Con la misma pena prevista en el apartado anterior serán castigados:

a) Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo.

b) Los que, para su utilización fraudulenta, sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo.

3. Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo.»

Ley 25/2007 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

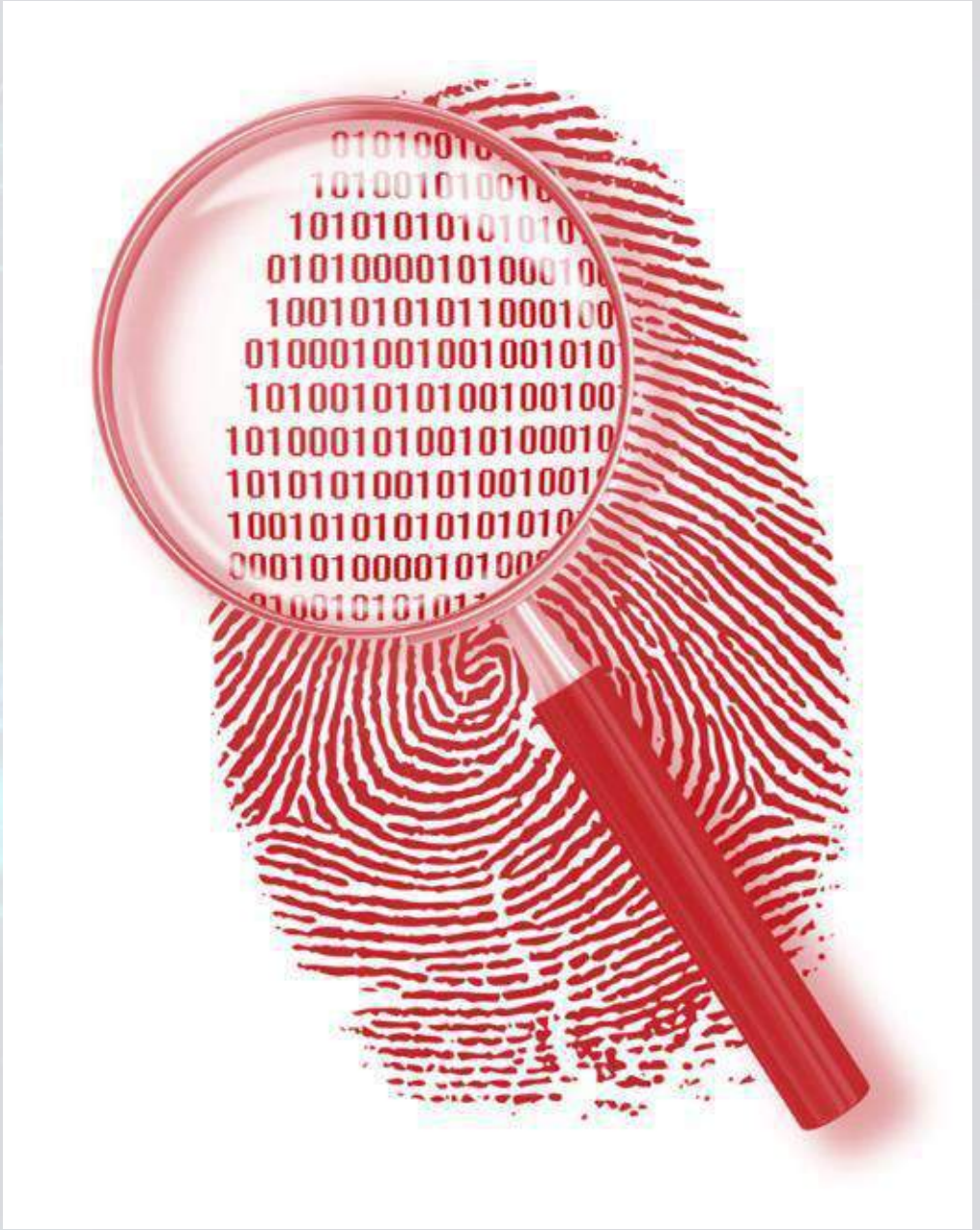
Artículo 5. *Periodo de conservación de los datos.*

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

Informática Forense

“El análisis forense es el proceso de identificar, preservar, analizar y presentar las evidencias de una forma legal y aceptable”.

(Rodney McKemmish 1999).



Evidencias.- Consideraciones legales

Admisibles	Deben ser conformes con las leyes actuales para que puedan ser presentadas ante un jurado en el caso de que sea necesario y tener un valor legal.
Auténticas	Deben estar autenticadas.
Completas	Deben ser objetivas y técnicas, en ningún caso una opinión personal para poder cumplir con el criterio de suficiencia.
Confiables	Se debe conocer con exactitud la procedencia de cada una de las evidencias.
Creíbles	Deben ser realmente demostrables y comprensibles para los miembros de un jurado.
Verificables	Deben poder comprobar la veracidad de cada una de ellas.

Es un protocolo de actuación diseñado para asegurar la integridad y veracidad de las evidencias, desde su origen hasta la presentación final.

Cadena de custodia

Cadena de custodia

- Documento que sirve para garantizar, ***sin ningún género de dudas,*** que el indicio incautado en el lugar de los hechos o durante el transcurso de una investigación, es el mismo que el que llegar al laboratorio.

- **Objetivos:**
  - Mantener la ***integridad*** de la evidencia
  - Asegurar la ***autenticidad*** de la misma
  - Garantizar la posibilidad de ***localización***
  - Permitir la ***trazabilidad*** de los accesos y acciones
  - Preservación a ***largo plazo***

Etapas


CADENA DE CUSTODIA
CONSERVACIÓN
IDENTIFICACIÓN
RECOGIDA
TRANSPORTE
ADQUISICIÓN
VERIFICACIÓN
ANÁLISIS
PROTECCIÓN
DISPOSICIÓN FINAL

Objetivos de los ciberdelincuentes

Objetivos de los ciberdelincuentes

1.- Dinero:

A través de los siguientes medios:

- **Datos de formularios.**
- **Envío no consentido de SMS Premium**
- **Extorsión**

Objetivos de los ciberdelincuentes

2.- Información

Recopilar datos alojados:

- **Datos de acceso.**
- **Datos y documentos privados.**
- **Control de recursos de procesamiento del equipo.**

Vectores de ataque de los ciberdelincuentes

Spam

Distribución:

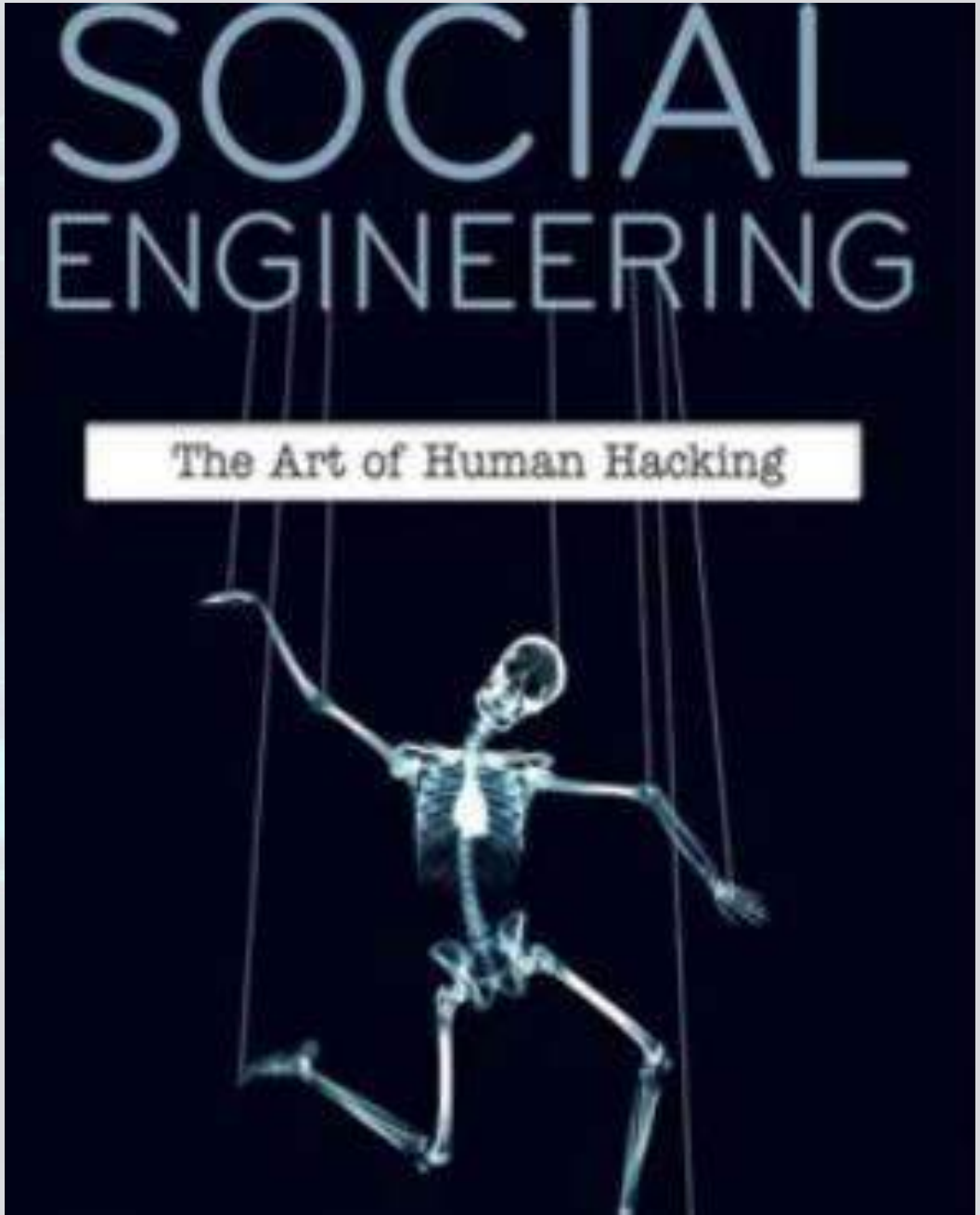
- **Listas de correo.**
- **Compra de bases de datos a particulares y empresas.**
- **Uso de robots que buscan direcciones en webs.**

Vectores de ataque de los ciberdelincuentes

INGENIERÍA SOCIAL

Es el arte de manipular a la gente para que haga lo que uno quiere.

Los usuarios son el eslabón débil



Vectores de ataque de los ciberdelincuentes

Vulnerabilidades

Malware multiplataforma

Vectores de ataque de los ciberdelincuentes

Dispositivos extraíbles

Vectores de ataque de los ciberdelincuentes


WIFI GRATIS