



LA CIBERDELINCUENCIA

TRATAMIENTO SUSTANTIVO (I)

CONVENIO DE BUDAPEST.

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
2. Delitos informáticos relacionados con el fraude y la falsificación
3. Delitos relacionados con el contenido
4. Delitos relacionados con infracciones a la propiedad intelectual y derechos afines

Protocolo Adicional:

1. Propaganda racista y xenófoba. Difundir material de odio a través de sistemas informáticos.
2. Amenazas e insultos por motivos racistas y xenófobos a través de medios informáticos

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

Estos delitos afectan la seguridad de la información almacenada o procesada en sistemas informáticos. Incluyen:

- **Acceso no autorizado (hacking):** Ingreso no autorizado a sistemas informáticos o bases de datos.
 - *Ejemplo:* Un hacker obtiene acceso a la base de datos de una empresa sin permiso.
- **Intercepción ilícita:** interceptación de datos o comunicaciones en transmisión sin autorización.
 - *Ejemplo:* Espionaje electrónico mediante el robo de información confidencial desde correos electrónicos.
- **Modificación o destrucción de datos:** Alteración, borrado o supresión de datos sin permiso.
 - *Ejemplo:* Un ciberdelincuente borra registros financieros de una empresa para encubrir fraudes.
- **Interferencia en el sistema:** Alteración, daño o interrupción del funcionamiento de un sistema informático.
 - *Ejemplo:* Un ataque de denegación de servicio (DDoS) contra un sitio web para bloquear su acceso.
- **Abuso de dispositivos:** Producción, venta o posesión de herramientas diseñadas para cometer ciberdelitos.
 - *Ejemplo:* Creación y distribución de malware o programas de hacking.

2. Delitos informáticos relacionados con el fraude y la falsificación

Se refieren a fraudes cometidos con medios digitales y la manipulación de información con intención de engañar.

- **Falsificación informática:** alteración o manipulación no autorizada de datos, generando datos no auténticos, p.e. con intención defraudatoria.
 - *Ejemplo:* Modificación de registros electrónicos para emitir facturas falsas.
- **Fraude informático:** estafas en línea o uso de sistemas informáticos para cometer fraude y obtener beneficios ilícitos.
 - *Ejemplo:* Un estafador crea una tienda en línea falsa y recibe pagos sin enviar los productos.

3. Delitos relacionados con el contenido

Este grupo incluye delitos en los que se utiliza la tecnología para distribuir material ilegal o perjudicial.

- **Pornografía infantil:** Producción, distribución, oferta, difusión, adquisición o posesión de material de abuso infantil en formato digital.
 - *Ejemplo: Intercambios de imágenes y videos de explotación sexual infantil.*

4. Delitos relacionados con infracciones a la propiedad intelectual y derechos afines

Se refiere a la violación de derechos de autor y distribución ilegal de contenido protegido.

- **Violación de derechos de autor:** Distribución o reproducción no autorizada de contenido protegido por copyright.

Ejemplo: Webs de descarga ilegal de películas, música o software sin pagar derechos de autor.

Características del Cibercrimen como Empresa ("crime as a service")

- Estrategias de ataque avanzadas
- Uso de inteligencia artificial y automatización para ataques masivos.
- Los grupos de cibercriminales operan como empresas: división de roles
- Ataques dirigidos a empresas con ingeniería social y phishing sofisticado.
- Espionaje corporativo: Venta de información confidencial robada.
- En mercados clandestinos (Dark Web) se venden datos robados, exploits y servicios de hacking.
- Operadores de ransomware: alquilan malware listo para usar y extorsionan a empresas tras cifrar sus datos: "Ransomware-as-a-Service" (RaaS)
- Lavado de capitales: las criptomonedas facilitan pagos anónimos sin rastreo.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.-

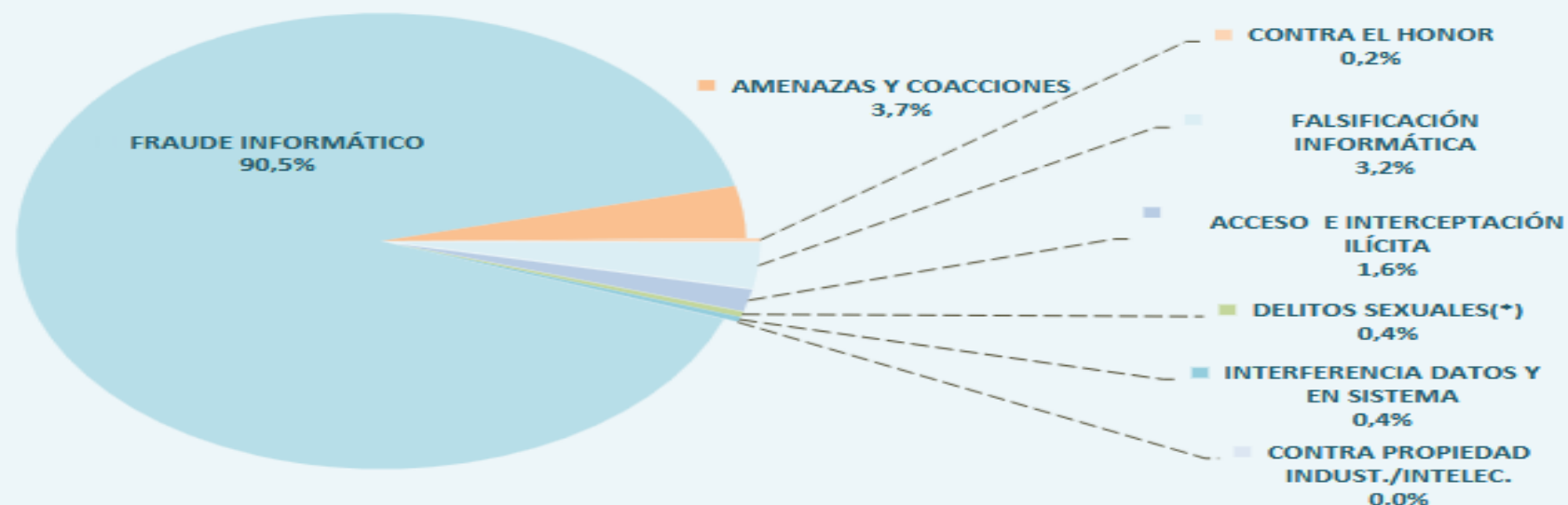
DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 3.1. Evolución de hechos conocidos por categorías delictivas

HECHOS CONOCIDOS	2019	2020	2021	2022	2023
ACCESO E INTERCEPTACIÓN ILÍCITA	4.004	4.653	5.342	5.578	7.367
AMENAZAS Y COACCIONES	12.782	14.066	17.319	15.982	17.472
CONTRA EL HONOR	1.422	1.550	1.426	1.191	1.174
CONTRA PROPIEDAD INDUST./INTELEC.	197	125	137	114	64
DELITOS SEXUALES(*)	1.774	1.783	1.628	1.646	1.804
FALSIFICACIÓN INFORMÁTICA	4.275	6.289	10.476	12.569	15.137
FRAUDE INFORMÁTICO	192.375	257.907	267.011	335.995	427.448
INTERFERENCIA DATOS Y EN SISTEMA	1.473	1.590	2.138	1.662	1.659
Total HECHOS CONOCIDOS	218.302	287.963	305.477	374.737	472.125

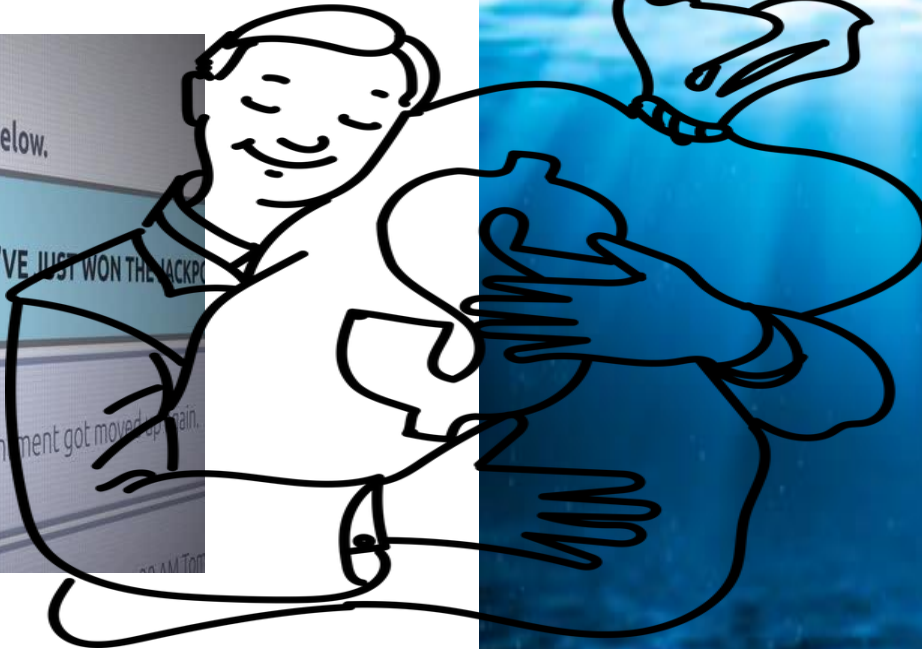
(*)Excluidas las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



Estafa informática (art. 8 Convenio de Budapest)



- Esquema tradicional: engaño-error
- Avances tecnológicos: globalización del comercio electrónico, banca online, criptomonedas, etc.
- Nuevos medios de pago distintos del dinero en efectivo.
- Ejs: ofertas de inversión de alta rentabilidad, lanzamiento de nuevas monedas virtuales, ventas engañosas, subastas fraudulentas en internet, clonación de tarjetas de crédito, etc.



UN DELITO, MUCHOS NOMBRES

EL FRAUDE **BUSINESS EMAIL COMPROMISE** PUEDE TENER OTROS NOMBRES – CUIDADO CON TODOS ELLOS



#BECareful

¿QUÉ ES **BUSINESS EMAIL COMPROMISE (BEC)**?



ACCESO ILEGAL

Los delincuentes acceden a los dispositivos o sistemas de las víctimas mediante piratería, sitios web de phishing o software malicioso, y posteriormente engañan a la víctima para que realice una transferencia de dinero a su cuenta bancaria.



INGENIERÍA SOCIAL

Los delincuentes eligen a sus víctimas basándose en la información que estas comparten en las plataformas de medios sociales.



SOLICITUDES URGENTES

El delincuente se hace pasar por un proveedor solicitando un pago urgente o el cambio de la información bancaria, o por un empleado de alto nivel en la empresa con autoridad para autorizar pagos.

#BECareful



INTERPOL

ANATOMÍA DEL «**B**USINESS **E**MAIL **C**OMPROMISE»

3 INGREDIENTES TÓXICOS

¡Bajo coste!
¡Bajo riesgo!
¡Alto índice de
rentabilidad!

1 Piratería

Una cuenta de correo electrónico se ve comprometida por software malicioso, intrusión de empleados, etc.

1

+

2

+

3

=

Beneficios ilegales millonarios

Fraude basado en ingeniería social

Se manipula a la víctima para que aporte información o fondos.

Blanqueo de capitales

Se realizan numerosas transferencias implicando a bancos o instituciones extranjeras

#BECareful

Estafa informática (art. 8 Convenio de Budapest)

- Beneficio económico para sí mismo o un tercero
- Perjuicio patrimonial a otro
- Intencionado
- Sin autorización



- ☐ Introducción, alteración, borrado o supresión de DATOS INFORMÁTICOS
- ☐ Cualquier forma de atentado al funcionamiento de un SISTEMA INFORMÁTICO
- Directiva 2019/713 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo I.

Artículo 249 Código Penal Español.

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:

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.

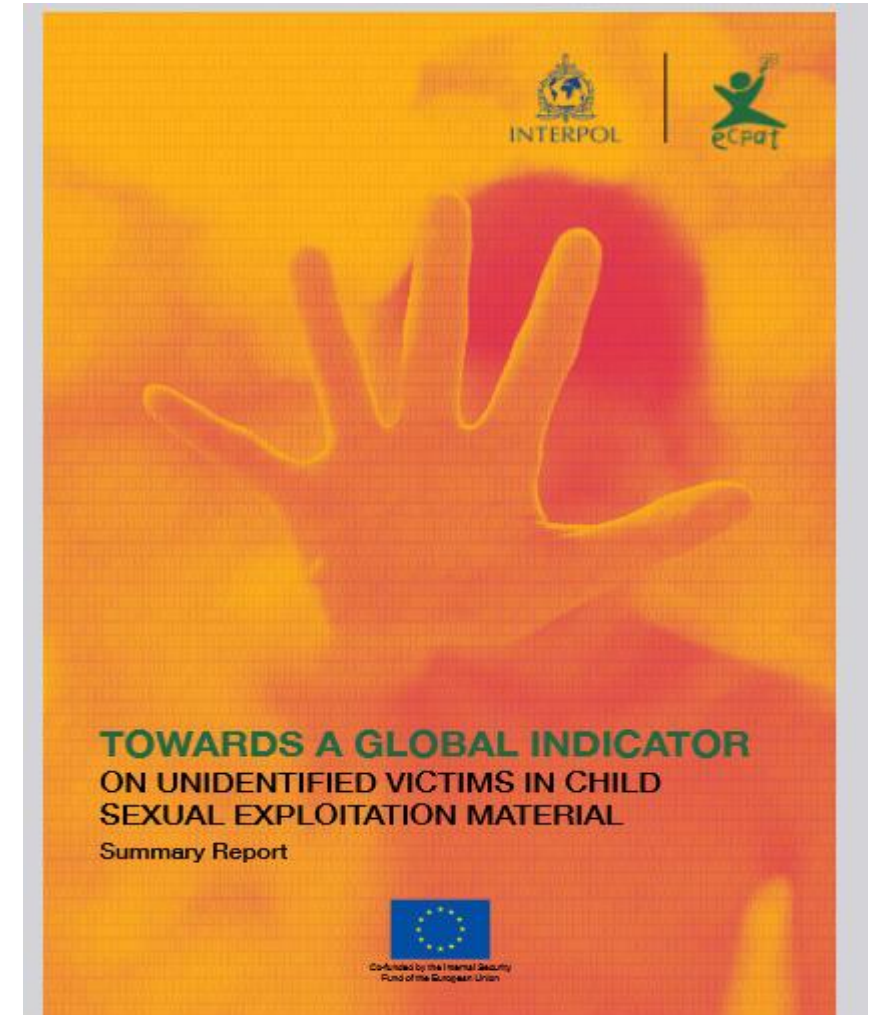
PORNOGRAFÍA INFANTIL (ART. 9 CONVENIO DE BUDAPEST)



Los pedófilos se refieren a niños como 'Caldo de Pollo' y en muchos casos son padres, según la Policía

El estudio identificó una serie de tendencias alarmantes:

- El 92 % de los agresores visibles eran hombres
- El 65 % de las víctimas no identificadas eran niñas.
- El 84 % de las imágenes contenía actividad sexual explícita.
- Más del 60 % de las víctimas no identificadas eran prepubescentes, inclusive bebés y niños pequeños.
- Cuanto más joven era la víctima, más grave era el abuso.
- En las imágenes de abusos graves era probable ver a niños, más que niñas.



Base de Datos Internacional de INTERPOL sobre Explotación Sexual de Niños

70



países conectados

14



víctimas identificadas
de media cada día



42 300

víctimas identificadas



18 300

delincuentes identificados

Julio de 2024

www.interpol.int



«pornografía infantil» se entenderá todo material pornográfico que contenga la representación visual de:

- a) Un menor comportándose de una forma sexualmente explícita;
- b) una persona que parezca un menor comportándose de una forma sexualmente explícita;
- c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

«menor» se entenderá toda persona menor de dieciocho años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de dieciséis años.

PORNOGRAFÍA INFANTIL (ART. 9 CONVENIO DE BUDAPEST)

➤ Intencionado

➤ Sin autorización

- a) La **producción** de pornografía infantil con vistas a su difusión por medio de un sistema informático;
- b) la **oferta o la puesta a disposición** de pornografía infantil por medio de un sistema informático;
- c) la **difusión o transmisión** de pornografía infantil por medio de un sistema informático,
- d) la **adquisición** de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;
- e) la **posesión** de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.



Art. 189,1 Código Penal Español.

A los efectos de este Título se considera pornografía infantil o en cuya elaboración hayan sido utilizadas **personas con discapacidad necesitadas de especial protección**:

- a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada.
- b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales.
- c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, **salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.**
- d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales.

Artículo 189 Código Penal Español.

1. Será castigado con la pena de prisión de uno a cinco años:

a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.

b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

2. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concorra alguna de las circunstancias siguientes:

- a) Cuando se utilice a **menores de dieciséis años**.
- b) Cuando los hechos revistan un carácter **particularmente degradante o vejatorio**, se emplee violencia física o **sexual** para la obtención del material pornográfico o se representen escenas de violencia física o sexual.
- c) Cuando se utilice a personas menores de edad que se hallen en una situación de **especial vulnerabilidad** por razón de enfermedad, discapacidad o por cualquier otra circunstancia.
- d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, **la vida o salud** de la víctima.
- e) Cuando el material pornográfico fuera de **notoria importancia**.
- f) Cuando el culpable perteneciere a una **organización o asociación**, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.
- g) Cuando el responsable sea **ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada**, de hecho, aunque fuera provisionalmente, o de derecho, de la persona menor de edad o persona con discapacidad necesitada de especial protección, o se trate de cualquier persona que conviva con él o de otra persona que haya actuado abusando de su posición reconocida de **confianza o autoridad**.
- h) Cuando concorra la agravante de **reincidencia**.

Art. 189 Código Penal Español

4. El que asistiere a sabiendas a espectáculos exhibicionistas o pornográficos en los que participen menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de seis meses a dos años de prisión.

5. El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.

La misma pena se impondrá a quien acceda a sabiendas a pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, **por medio de las tecnologías de la información y la comunicación**



Artículo 189 bis.

La distribución o difusión pública a través de Internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos específicamente destinados a promover, fomentar o incitar a la comisión de los delitos previstos en este capítulo y en los capítulos II y IV del presente título será castigada con la pena de multa de seis a doce meses o pena de prisión de uno a tres años.



CHILDGROOMING



- Declaración de Rio Janeiro y Llamado a la acción para prevenir y detener la explotación sexual de niños, niñas y adolescentes.
- Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual
- Directiva 2011/93/CE relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.

➤ Artículo 183 Código Penal Español.

1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación **contacte con un menor de dieciséis años y proponga concertar un encuentro** con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 181 y 189, siempre que tal propuesta se acompañe de **actos materiales encaminados al acercamiento**, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, **sin perjuicio de las penas correspondientes a los delitos en su caso cometidos.**

Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante **coacción, intimidación o engaño.**

2. El que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación **contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle** para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años.

SEXTORSION. DISTRIBUCIÓN NO CONSENTIDA DE IMÁGENES ÍNTIMAS

ART. 197,7 Código Penal Español



7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, **difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia** en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación **menoscabe gravemente la intimidad personal** de esa persona.

Se impondrá la pena de multa de uno a tres meses a quien habiendo recibido las imágenes o grabaciones audiovisuales a las que se refiere el párrafo anterior las **difunda, revele o ceda a terceros** sin el consentimiento de la persona afectada.

En los supuestos de los párrafos anteriores, la pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el **cónyuge** o por persona que esté o haya estado unida a él por **análoga relación de afectividad**, aun sin convivencia, la víctima fuera **menor** de edad o una **persona con discapacidad necesitada de especial protección**, o los hechos se hubieran cometido con una **finalidad lucrativa**.

CIBERACOSO

Directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica.

Artículo 6. Ciberacecho

Los Estados miembros garantizarán que sea punible como delito la conducta intencionada de someter reiterada o continuamente a otra persona a vigilancia, sin el consentimiento de esa persona o una autorización legal para hacerlo, mediante TIC, a fin de rastrear u observar los movimientos y actividades de dicha persona, cuando sea probable que tal conducta cause graves daños a esa persona.

Artículo 7. Ciberacoso

Los Estados miembros garantizarán que las siguientes conductas intencionadas sean punibles como delito:

- a) la participación reiterada o continua en conductas amenazantes dirigidas contra otra persona, al menos cuando esa conducta implique amenazas de cometer delitos, mediante TIC, y cuando sea probable que cause en la persona un profundo temor por su propia seguridad o por la seguridad de las personas a cargo;
- b) la participación, junto con otras personas, mediante TIC, en conductas amenazantes o insultantes accesibles públicamente dirigidas contra una persona, cuando sea probable que tal conducta cause graves daños psicológicos a esa persona;
- c) el envío no solicitado a una persona, mediante TIC, de una imagen, vídeo u otro material similar que represente los genitales, cuando sea probable que tal conducta cause daños psicológicos a esa persona;
- d) hacer accesible al público, mediante TIC, material que contenga los datos personales de una persona, sin su consentimiento, con el fin de incitar a terceros a causar lesiones físicas o psicológicas graves a dicha persona.



➤ Artículo 172 ter Código Penal Español.

1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que **acose a una persona llevando a cabo de forma insistente y reiterada**, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de esta forma, **altere el normal desarrollo de su vida cotidiana**:

1.ª La vigile, la persiga o busque su cercanía física.

2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

-
- sin perjuicio de las penas que pudieran corresponder a los **actos concretos de acoso**.
 - sólo serán perseguibles mediante denuncia de la persona agraviada o de su representante legal.
 - **Agravación:** cónyuge o análoga relación de afectividad aun sin convivencia, o sobre los descendientes, ascendientes o hermanos, propios o del cónyuge o conviviente, o sobre los menores o personas con discapacidad necesitadas de especial protección que con él convivan o que se hallen sujetos a la potestad, tutela, curatela, acogimiento o guarda de hecho del cónyuge o conviviente, o sobre persona amparada en cualquier otra relación por la que se encuentre integrada en el núcleo de su convivencia familiar, así como sobre las personas que por su especial vulnerabilidad se encuentran sometidas a custodia o guarda en centros públicos o privados. En este caso no será necesaria denuncia del ofendido.

Art. 172 ter, 5 Código Penal Español

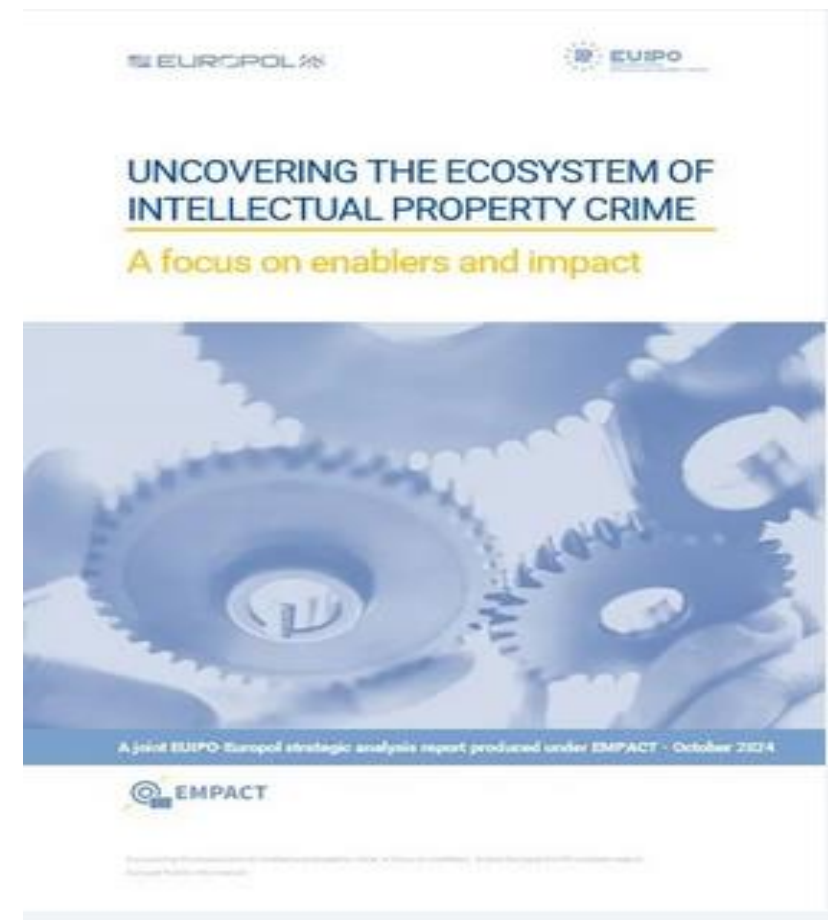
5. El que, sin consentimiento de su titular, **utilice la imagen de una persona** para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la misma **situación de acoso, hostigamiento o humillación**, será castigado con pena de prisión de tres meses a un año o multa de seis a doce meses.

Si la víctima del delito es un menor o una persona con discapacidad, se aplicará la mitad superior de la condena.



PROPIEDAD INTELECTUAL (ART. 10 CONVENIO DE BUDAPEST)

- Intencionado
- A escala comercial
- Derechos de propiedad intelectual y derechos afines
- Remisión a la legislación nacional





Counterfeiting and piracy

- Fake goods: foodstuff, medicines, toys, pesticides, etc.
- Illegal supply of digital content: music, films, software



Links with:

- Organised crime
- Drug trafficking
- Forced labour
- Cybercrime
- Money laundering



Consequences:

- Financial loss and tax evasion
- Risk to consumer's health
- Reputational damage
- Environmental impact

Artículo 270 Código Penal Español.

1. Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, **reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente**, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, **sin la autorización** de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.
2. La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, **facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico**, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual **sin la autorización** de los titulares de los correspondientes derechos o de sus cesionarios, **en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos** referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios.

Art. 270,5 Código penal Español

c) **Favorezcan o faciliten la realización de las conductas** a que se refieren los apartados 1 y 2 de este artículo **eliminando o modificando**, sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, **las medidas tecnológicas eficaces** incorporadas por éstos con la finalidad de impedir o restringir su realización.

d) Con ánimo de obtener un beneficio económico directo o indirecto, **con la finalidad de facilitar a terceros el acceso** a un ejemplar de una obra literaria, artística o científica, o a su transformación, interpretación o ejecución artística, fijada en cualquier tipo de soporte o comunicado a través de cualquier medio, y sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, **eluda o facilite la elusión de las medidas tecnológicas eficaces dispuestas para evitarlo.**

6. Será castigado también con una pena de prisión de seis meses a tres años quien fabrique, importe, **ponga en circulación o posea con una finalidad comercial** cualquier medio principalmente concebido, producido, adaptado o realizado para **facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico** que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en los dos primeros apartados de este artículo.

ATAQUES A DATOS Y SISTEMAS DE INFORMACIÓN (ART. 2 A 6 CONVENIO DE BUDAPEST)

- Bien jurídico protegido: **disponibilidad, integridad y confidencialidad datos informáticos.**
 - Intencionado
 - Sin autorización
-
- ☐ Acceso ilícito (art. 2)
 - ☐ Interceptación ilícita (art. 3)
 - ☐ Atentados contra la integridad de los datos (art. 4)
 - ☐ Atentados contra la integridad de los sistemas informáticos (art. 5)
 - ☐ Abuso de equipos e instrumentos técnicos (art. 6)



Artículo 264 Código Penal español.

1. El que por cualquier medio, sin autorización y de manera grave **borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles** datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera **grave**, será castigado con la pena de prisión de seis meses a tres años.

1.ª Se hubiese cometido en el marco de una **organización criminal**.

2.ª Haya ocasionado daños de **especial gravedad** o afectado a un **número elevado de sistemas informáticos**.

3.ª El hecho hubiera **perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad**.

4.ª Los hechos hayan afectado al sistema informático de una **infraestructura crítica** o se hubiera creado una situación de **peligro grave para la seguridad** del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

Si los hechos hubieran resultado de **extrema gravedad**, podrá imponerse la pena superior en grado

Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la **utilización ilícita de datos personales de otra persona** para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Artículo 264 bis Código Penal Español.

1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera **grave**, **obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno**:

- a) realizando alguna de las **conductas** a que se refiere el artículo anterior;
- b) **introduciendo o transmitiendo datos**; o
- c) **destruyendo, dañando, inutilizando, eliminando o sustituyendo** un sistema informático, telemático o de almacenamiento de información electrónica.

Si los hechos hubieran **perjudicado de forma relevante la actividad normal** de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.

Artículo 264 ter Código Penal Español.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, **produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros**, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

- a) un **programa informático**, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o
- b) una **contraseña** de ordenador, un **código de acceso** o **datos similares** que permitan acceder a la totalidad o a una parte de un sistema de información.

DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

➤ ART. 197 Código Penal Español

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, **intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación**, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, **se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro** que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, **acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.**

ESPIONAJE CIBERNÉTICO

Artículo 197 bis Código Penal Español

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, **acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad** de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.
2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, **intercepte transmisiones no públicas de datos informáticos** que se produzcan desde, hacia o dentro de un sistema de información, incluidas las **emisiones electromagnéticas** de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Artículo 197 ter Código Penal Español.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, **produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros**, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

- a) un **programa informático**, concebido o adaptado principalmente para cometer dichos delitos; o
- b) una **contraseña de ordenador, un código de acceso o datos similares** que permitan acceder a la totalidad o a una parte de un sistema de información.

Convención de las Naciones Unidas contra la Ciberdelincuencia (2024)



- ☐ Acceso ilícito (art.7)
- ☐ Interceptación ilícita (art. 8)
- ☐ Interferencia con datos electrónicos (art. 9)
- ☐ Interferencia con un sistema de tecnología de la información y las comunicaciones (art. 10)
- ☐ Uso indebido de dispositivos (art. 11)
- ☐ Falsificación relacionada con un sistema de tecnología de la información y las comunicaciones (art. 12)
- ☐ Robo o fraude relacionados con un sistema de tecnología de la información y las comunicaciones (art. 13)
- ☐ Delitos relacionados con material en línea que muestra abusos sexuales de niños o explotación sexual de niños (art. 14)
- ☐ Instigación o captación con el fin de cometer un delito sexual contra un niño (art. 15)
- ☐ Difusión no consentida de imágenes de carácter íntimo (art. 16)
- ☐ Blanqueo del producto del delito (art. 17)

- ☐ Responsabilidad de las personas jurídicas (art. 18)
- ☐ Participación y tentativa (art. 19)



GRACIAS

JM.SANCHEZ.S@PODERJUDICIAL.ES