DELITOS INFORMÁTICOS

PASO A PASO

Análisis detallado de las conductas delictivas más comunes en el entorno informático

Coordinadora de la obra
ESCARLATA GUTIÉRREZ MAYO
Fiscal adjunta a la Sección contra la Criminalidad Informática en la Fiscalía Provincial de Ciudad Real

1.ª EDICIÓN 2021
Incluye formularios

COLEX READER

COLEX

DELITOS INFORMÁTICOS

Análisis detallado de las conductas delictivas más comunes en el entorno informático

1.ª EDICIÓN 2021

Obra realizada por el Departamento de Documentación de Iberley

Coordinadora

Escarlata Gutiérrez Mayo

Fiscal adjunta a la Sección contra la Criminalidad Informática en la Fiscalía Provincial de Ciudad Real

Colaboradoras

M.ª Virginia Castro Romero

Iria Pérez Golpe

COLEX 2021

© Editorial Colex, S.L.
Calle Costa Rica, número 5, 3.º B (local comercial)
A Coruña, 15004, A Coruña (Galicia)
info@colex.es
www.colex.es

I.S.B.N.: 978-84-1359-257-2
Depósito legal: C 893-2021

SUMARIO

1. INTRODUCCIÓN 9

2. RETOS Y DESAFÍOS QUE PLANTEAN ESTOS DELITOS 19

3. ESTAFA INFORMÁTICA: ARTÍCULO 248.2 CP 23

4. *PHISHING* 43

5. DAÑOS INFORMÁTICOS 51

6. *STALKING:* ARTÍCULO 172 TER CP 65

7. DELITOS CONTRA LA INTIMIDAD 75
7.1. Tipo básico: artículo 197.1 y 3 CP 76
7.2. *Sexting:* tipo del artículo 197.7 CP 91
7.3. Delito de acceso ilegal a sistemas informáticos: art. 197. bis 1 CP 95
7.4. Delito de abuso de dispositivos (uso de programas espía): art. 197 ter CP 101
7.5. Agravaciones: art. 197 quater CP 104
7.6. Responsabilidad penal de las personas jurídicas: art. 197 quinquies CP 106
7.7. Requisito de perseguibilidad y perdón del ofendido 111

8. *CHILDGROOMING:* ARTÍCULO 183 TER 2 CP 115

9. DIFUSIÓN Y POSESIÓN DE PORNOGRAFÍA INFANTIL: ARTÍCULO 189.1 Y 5 CP 121

10. LA PRUEBA DIGITAL 127

ANEXO. FORMULARIOS

Denuncia por delito de childgrooming del artículo 183 ter CP (ciberacoso a menores) 137

Denuncia delito de acoso o *stalking* regulado en el artículo 172 ter CP 139

Querella por delito de daños informáticos del artículo 264 C.P. 141

Querella por delito de daños informáticos por obstaculización o interrupción del funcionamiento de un sistema informático ajeno (artículo 264 bis CP) 145

Denuncia por delito de estafa informática tipificado en el artículo 248.2 CP *(phishing)* 149

Querella por delito contra la intimidad sexual *(sexting)* del artículo 197.7 CP 151

Querella por delito de descubrimiento y revelación de secretos del artículo 197 CP . .155

Querella por delito de acceso ilícito a un sistema informático, mediante las conductas del artículo 197 ter CP 163

Denuncia por delito relativo a la difusión y posesión de pornografía infantil del artículo 189.5 CP 167

1.
INTRODUCCIÓN

Hacia la conceptualización del «delito informático»

Para acercarnos al estudio del delito informático es fundamental hacer un encuadre general esto es, conocer en base a qué preceptos emana y encuentra su argumento la antijuridicidad de este tipo de actos. Acudiendo a la norma suprema de nuestro ordenamiento:

> Artículo 18 C.E.
>
> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
>
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
>
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
>
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

A TENER EN CUENTA. Los derechos de los apartados 2 y 3 del artículo 18 C.E. pueden ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio o pueden ser suspendidos (mediante LO, bajo intervención judicial y control parlamentario) a determinadas personas en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas, todo ello al amparo de lo previsto en el artículo 55 de la Constitución Española.

Tribunal Constitucional y Tribunal Supremo han hecho una interpretación importante al respecto de este precepto constitucional, tanto del **derecho a la intimidad en sentido genérico como del derecho a la intimidad confluyendo con la libertad informática:**

STC n.º 134/1999, de 15 de julio, ECLI:ES:TC:1999:134

«El derecho a la intimidad salvaguardado en el art. 18.1 C.E. tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y al conocimiento de terceros, sean estos poderes públicos o simples particulares, que está ligado al respeto de su dignidad (...)».

STS n.º 553/2015, de 6 de octubre, ECLI:ES:TS:2015:4054

«Del precepto constitucional se deduce que el derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a su persona o a la de su familia, pudiendo imponer a terceros su voluntad de no dar a conocer dicha información o prohibiendo su difusión no consentida, lo que ha de encontrar sus límites, como es obvio, en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos (...)».

STS n.º 553/2015, de 6 de octubre, ECLI:ES:TS:2015:4054

«En este sentido los derechos a la intimidad personal y a la propia imagen garantizados por el art. 18.1 CE, forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida privada. Salvaguardan estos derechos un espacio de intimidad personal y familiar que queda sustraído a intromisiones extrañas, destacando la necesaria protección frente al creciente desarrollo de los medios y procedimiento de captación, divulgación y difusión de la misma y de datos y circunstancias que pertenecen a la intimidad.

Por intimidad, por tanto, se pueden entender diversos conceptos, siendo significativo a estos efectos que la terminología usada para referirse a dicho concepto varia en los distintos países (...), pero que vienen a coincidir en la existencia de una esfera de privacidad que cabe considerar secreto en el sentido de ser facultad de la persona su exclusión del conocimiento de terceros. El Código actual ha hecho además especial referencia a la llamada 'libertad informática, ante la necesidad de conceder a la persona facultades de control sobre sus datos en una sociedad informatizada, siguiendo las pautas de la Ley Orgánica de Regulación del tratamiento Automatizado de Datos personas (LORTAD) 5/92 de 29.10, relacionada con el Convenio del Consejo de Europa de 28.1.81, y la Directiva 95/46 del Parlamento de la Unión Europea relativos a la protección de tales datos y a su libre circulación.

Esta segunda dimensión de la intimidad conocida como libertad informática o habeas data, encuentra su apoyo en el art. 18.4 CE, en donde taxativamente se dispone que 'la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos'. De esta proclamación se deriva su poder de acción del titular para exigir que determinados datos personales no sean conocidos, lo que supone reconocer un derecho a la autodeterminación informativa, entendido como libertad de decidir qué datos personales pueden ser obtenidos y tratados por otros. La llamada libertad informática significa, pues, el derecho a controlar el uso de los datos de carácter personal y familiar que pueden recogerse y tratarse informáticamente (habeas data); en particular –como señala la doctrina– entre otros aspectos, la capacidad del ciudadano para oponerse a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención (...)».

En el mismo sentido, y como antesala a lo que justificará la regulación del delito informático, cabe mencionar la **normativa internacional y europea** que, a lo largo de la historia, ha consagrado estos derechos y, de manera especial, el **derecho de toda persona a no ser objeto de injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia o ser violada o atacada su honra o reputación:**

- **Declaración Universal de Derechos Humanos** de 10 de diciembre de 1948 (art. 12).
- **Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales** de 4 de noviembre de 1950 (art. 8).

- **Pacto Internacional de Derechos Civiles y Políticos** de 19 de diciembre de 1966 (art. 17).
- **Pacto Internacional de Derechos Económicos, Sociales y Culturales** de 19 de diciembre de 1966.
- **Convención de las Naciones Unidas sobre los Derechos del Niño (1989)**.
- **Convenio Internacional del Trabajo sobre las peores formas de trabajo de los menores (1999)**.
- **Convenio sobre la Ciberdelincuencia, celebrado en Budapest el 23 de noviembre de 2001**.
- **Directiva 2013/40/UE, de 12 de agosto** relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.
- Reglas mínimas de las Naciones Unidas para la administración de la justicia de menores (***«Reglas de Beijing»***), adoptadas por la Asamblea General en su resolución 40/33, de 28 de noviembre de 1985 cuyo objetivo es promover el bien del menor y de su familia, debiendo los Estados Miembros promover medidas a tal efecto.
- **Acuerdo de Schengen**, que suprime los controles en fronteras interiores entre países de Europa firmantes.

Asimismo, y como profundizaremos en las líneas siguientes, en cuanto a **legislación y normativa nacional** aplicable a asuntos relativos a delitos informáticos, debemos citar:

- **Ley Orgánica 1/1982, de 5 de mayo**, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- **Ley 10/1995, de 23 de noviembre, del Código Penal**.
- **Ley Orgánica 5/2000, de 12 de enero**, reguladora de la responsabilidad penal de los menores que se aplicará para exigir la responsabilidad de las personas mayores de 14 años y menores de 18 por la comisión de hechos tipificados como delito en el Código Penal o leyes especiales.
- **Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico** que establece el régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios.
- **Ley Orgánica 8/2015, de 22 de julio**, de modificación del sistema de protección a la infancia y a la adolescencia.
- **Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, que modifica la LO 1/1996 de Protección Jurídica del Menor**, de modificación parcial del código Civil y de la Ley de Enjuiciamiento Civil que viene a regular sobre el derecho de los menores a buscar, recibir y utilizar la información adecuada a su desarrollo prestando atención a la alfabetización digital y mediática adaptada a la etapa evolutiva del menor.
- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales** que da un amplio desarrollo al artículo 18.4 de la C.E.

- **Ley Orgánica 1/2015, de 30 de marzo**, por la que se **modifica** la Ley Orgánica 10/1995, de 23 de noviembre, del **Código Penal**.

Como **doctrina,** es determinante traer a colación:

- **La Circular 3/2017, de 21 de septiembre**, de la Fiscalía General del Estado, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, **en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos**.
- Con fecha anterior, pero fundamental para conocer ciertos conceptos concurrentes en el delito informático: la **Circular 2/2011, de 2 de junio**, de la Fiscalía General del Estado sobre la reforma del Código Penal por Ley Orgánica 5/2010 **en relación con las organizaciones y grupos criminales**.

Novedades en el Código Penal tras la reforma de la LO 1/2015 de 30 de marzo

Atendiendo a lo anterior, si bien en el artículo 18 de la Constitución Española se garantiza el derecho al honor, intimidad personal y familiar y a la propia imagen, limitando a tal fin el uso de la informática mediante ley, la «tipificación» del delito informático (aunque no hay una tipificación de este delito como tal en el Código Penal) no viene a ser más que un instrumento a través del cual hacer valer este derecho fundamental y protegerlo ante su posible vulneración.

> A TENER EN CUENTA. El «delito informático» no ha sido introducido por la LO 1/2015, de 30 de marzo, y no existe como tal, se trata más bien de un delito cometido a través de las TIC como herramienta, que plantea una serie de retos y peculiaridades.

La **Ley Orgánica 1/2015, de 30 de marzo** se elaboró respondiendo a la normativa europea reguladora de la delincuencia informática, llevando a cabo la transposición de la **Directiva 2013/40/UE, de 12 de agosto** relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos, cuando no se trata de una comunicación personal.

Así, como recoge el Preámbulo de la citada Ley Orgánica, de acuerdo con la Directiva europea, con ella se introduce una separación clara entre los supuestos de revelación de datos que afectan a la intimidad personal y el acceso a otros datos o informaciones que pueden afectar a la privacidad, pero que no se refieren a la intimidad personal; se tipifica la facilitación o producción de programas informáticos diseñados para la comisión de delitos de este tipo; y se prevé la responsabilidad de las personas jurídicas.

De esta forma, nuestro Código Penal adoptó un nuevo contenido, introduciéndose novedades en su articulado, con la incorporación de modificaciones y otras redacciones. En lo relativo a los delitos informáticos, cabe citar:

- La inserción del artículo 172 ter C.P. que introduce la figura del delito de acoso, con inciso sobre su comisión a través de cualquier medio de comunicación.
- Sobre los delitos de **abusos y agresiones sexuales a menores de 16 años**, destacar **el artículo 183 ter, apartado 2, del C.P.** que dispone sobre el de-

lito de *childgrooming* o acoso sexual a menores, así como lo preceptuado en **el artículo 189 del C.P.** que condena el delito relativo a la **difusión y posesión de pornografía infantil**.

- También dentro del Título X, Capítulo I del C.P., que regula los delitos relativos al descubrimiento y revelación de secretos, la LO 1/2015, de 30 de marzo supuso cambios en algunos de sus preceptos, como es el **artículo 197 del C.P., que en su apartado 1 viene a establecer**:

> «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».

- Y, sin perjuicio de la importancia que cubren los otros apartados del precepto anterior, debemos mencionar el **artículo 197.7 C.P.** que establece la siguiente agravante para la comisión del delito de ***sexting***:

> «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.
>
> 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».

- Otras novedades son el encaje de **los artículos 197 bis a 197 quinquies C.P.** que, con atención a especiales concreciones, regulan el **delito de acceso ilegal a sistemas informáticos, el delito de interceptación de dispositivos (programas espía),** las agravaciones para estos tipos, así como la **responsabilidad penal de las personas jurídicas** que cometan estos delitos.

- Importante también es la modificación introducida sobre el **artículo 264 C.P. que contempla el delito de daños informáticos**, así como la incorporación a la norma penal del artículo **264 quater**, con el fin de regular específicamente la pena en ese delito si **el responsable es una persona jurídica**.

DOCTRINA

La Fiscalía General del Estado, en la Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos asentó doctrina al respecto, dictando:

«Según se hace constar en el Preámbulo, siguiendo con ello el propio planteamiento de la Directiva europea, se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal y el acceso a otros datos o infor-

maciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal; no es lo mismo el acceso al listado personal de contactos que recabar datos relativos a la versión del "software" empleado o a la situación de los puertos de entrada a un sistema. Por ello se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos.

La decisión de sancionar separadamente el acceso ilegal a sistemas, adoptada por el Legislador ha de considerarse acertada, ya que su anterior ubicación resultaba perturbadora en la interpretación y aplicación de este tipo penal. Es evidente que en estos casos el bien jurídico protegido, no es directamente la intimidad personal, sino más bien la seguridad de los sistemas de información en cuanto medida de protección del ámbito de privacidad reservado a la posibilidad de conocimiento público. Lo que sanciona este precepto es el mero acceso a un sistema vulnerando las medidas de seguridad y sin estar autorizado para ello, sin que se exija que dicha conducta permita, de lugar, o posibilite en alguna forma el conocimiento de información de carácter íntimo o reservado. Con la tipificación en un precepto independiente se solventa la incongruencia, denunciada por buena parte de la doctrina, de sancionar esta conducta en el marco de un tipo penal definido por el dolo específico de descubrir los secretos o vulnerar la intimidad de otro.

(...)

Lo que el Legislador pretende sancionar más gravemente son aquellas conductas en las que el autor del hecho no solo invade intencionadamente la intimidad de una persona, cometiendo alguna de las conductas típicas, sino que además lleva a efecto dicho comportamiento haciendo uso de las señas de identidad propias de la víctima, es decir, haciéndose pasar por ella como medio para lograr sus criminales propósitos.

(...)

Como ya se ha indicado, el precepto se refiere a los supuestos de utilización de datos personales. Como tales han de entenderse no solo los datos de identidad oficial, en sentido estricto, sino cualesquiera que sean propios de una persona o utilizados por ella y que la identifiquen o hagan posible esa identificación frente a terceros tanto en un entorno físico como virtual. A los efectos de integrar este concepto, el art. 3 a) de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, define los datos de carácter personal como cualquier información concerniente a personas físicas identificadas o identificables, definición que se complementa con el art. 5.1 f) del Reglamento que desarrolla tal Ley Orgánica, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que entiende por tales cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier tipo concerniente a personas físicas identificadas o identificables. El mismo Reglamento proporciona en el apartado 5.1 o) el concepto de persona identificable describiéndola como toda persona cuya identidad pueda determinarse directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados».

Conceptos básicos en el delito informático

El **Convenio sobre la Ciberdelincuencia,** celebrado en Budapest el 23 de noviembre de 2001, nos acerca, en **su artículo 1,** una serie de **definiciones** como:

- **Sistema informático**: cualquier dispositivo aislado o en conjunto, interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa.

- **Datos informáticos**: 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.

- **Proveedor de servicios**: puede ser una entidad pública o privada que ofrezca a sus usuarios la opción de comunicar por medio de un sistema informático, o cualquier otro tipo de entidad que procese o almacene datos informáticos para el servicio de comunicación o usuarios de ese servicio.

- **Datos sobre el tráfico**: datos informáticos relativos a una comunicación por medio de un sistema informático y generados por un sistema de ese tipo, que indican el origen, destino, ruta, hora, fecha, tamaño, duración de la comunicación o tipo de servicio subyacente.

Con posterioridad, y con base en el referido Convenio, en la **Directiva 2013/40/UE, de 12 de agosto de 2013,** relativa a los ataques contra los sistemas de información, **artículo 2**, encontramos los siguientes conceptos, perfectamente definidos, que marcan las líneas básicas para detectar el delito informático. **Coincidiendo**, casi de manera literal, con el Convenio de Budapest en la descripción de los términos ***«sistema de información»*** y ***«datos informáticos»***, añade dos más:

- **Persona jurídica**: entidad reconocida como tal, a excepción de los Estados y otros organismos públicos que ejercen prerrogativas públicas y las organizaciones internacionales de carácter público.

- **Sin autorización**: un comportamiento que supone el acceso, la interferencia o la interceptación, sin autorización por el propietario u otro titular del derecho sobre el sistema o parte del mismo, o que simplemente no esté permitido por la ley estatal aplicable.

También es importante relacionar los diferentes **sujetos que interactúan en el mundo informático y que** pueden encajar, en ocasiones, como autores de este tipo de delito, pudiendo concurrir en el mismo diferentes perfiles como: *hacker, cracker, phreaker, lammers, gurús, newbie, bucaneros, trashing...*, y siendo siempre el **sujeto pasivo** la víctima, es decir, el usuario del sistema automatizado afectado.

Asimismo, los sujetos responsables de estos actos dañinos informáticos disponen de diferentes técnicas para poder lograr sus fines fraudulentos. Recibe el nombre de ***malwares*** y bajo este concepto se encajan innumerables *softwares* maliciosos (troyanos, virus, *phishing, spam, hoax, adware, spyware,* gusanos...), que se encuentran en continua creación y renovación para resistir a los programas de antivirus y demás sistemas utilizados en el mundo informático para combatirlos y eliminarlos.

DELITOS INFORMÁTICOS PASO A PASO

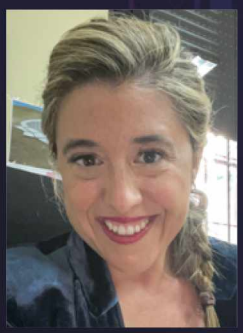
¿Qué es un delito informático?

¿Qué conductas punibles puede abarcar este tipo penal?

¿Qué especialidades presenta la prueba digital?

La respuesta a estas y otras preguntas podrán encontrarla en la presente guía, en la que se realiza un estudio pormenorizado de las normas penales relacionadas con la esfera digital. En esta obra son tratados de forma detallada, entre otros, delitos como la estafa informática, el delito de daños informáticos, el delito de *stalking*, el delito de *childgrooming* o el denominado *sexting*.

En el contenido se incluyen numerosas cuestiones prácticas, jurisprudencia relevante y formularios actualizados que ayudarán al lector a alcanzar una visión global del delito informático.



ESCARLATA GUTIÉRREZ MAYO

Escarlata Gutiérrez Mayo, Abogada-Fiscal de la Fiscalía Provincial de Ciudad Real. ST de Manzanares desde 2013. Adjunta a las Secciones contra la criminalidad informática y contra la delincuencia económica.

Ha publicado diversos artículos jurídicos y ha participado en obras colectivas sobre delitos cometidos a través de las TIC. Ha codirigido cursos en la Fiscalía Superior de CLM y en el Centro de Estudios Jurídicos del Ministerio de Justicia. Ha impartido ponencias en el CGPJ, en el CEJ y en diversas Universidades.

Igualmente está muy implicada en la divulgación jurídica a través de sus cuentas en Twitter @escar_gm, en Instagram @escarlata.gutierrez y en su canal de Youtube: Vídeos Jurídicos.

www.colex.es

COLEX

COLEX READER

PVP 19,00 €

ISBN: 978-84-1359-257-2

9 788413 592572