Derecho penal e Internet

Esther Morón Lerma

PID_00175358

Universitat Oberta de Catalunya

Índice

Introducción..... 5

Objetivos..... 7

1. Prevención y sanción de delitos vinculados a Internet..... 9

2. Responsabilidad administrativa y responsabilidad penal..... 11

3. Necesidad de distinción de contenidos en Internet..... 13

4. La errónea noción de delito informático..... 16

5. Delitos vinculados a la criminalidad informática en el Código penal español..... 18
5.1. Delitos contra la intimidad (arts. 197 a 200 CP) 18
5.1.1. Interceptación del correo electrónico del trabajador 19
5.2. Delito de fraude informático (art. 248.2 CP) 22
5.3. Delito de utilización abusiva de equipos (art. 256 CP) 24
5.4. Delito de daños informáticos (art. 264 CP) 24
5.5. Delitos contra la propiedad intelectual (art. 270 CP) 26
5.6. Delitos contra los secretos de empresa (art. 278.1 CP) 29
5.7. Delitos contra los intereses económicos de los prestadores de servicios (art. 286 CP) 30
5.8. Delitos vinculados a la pornografía infantil (art. 183 bis y 189 CP) 30
5.9. Otros ilícitos penales 32
5.10. Las conductas de *hacking* o de accesos inconsentidos a sistemas 32
5.10.1. Definición de la conducta de *hacking* (*white hacking*) 32
5.10.2. Encaje en el Código penal español, con carácter previo a la reforma de 2010 35
5.10.3. La regulación de estas conductas en la Unión Europea 37
5.10.4. El nuevo delito del art. 197.3 del Código penal 38

Resumen..... 41

Actividades..... 43

Ejercicios de autoevaluación..... 43

Solucionario..... 44

Glosario..... 45

Bibliografía..... 46

Introducción

El objetivo principal de este módulo se cifra en facilitar los conocimientos necesarios para que un profesional de la informática (un administrador de sistemas, por ejemplo) sepa cuáles son las obligaciones y, por tanto, las responsabilidades en las que puede incurrir a causa de su trabajo. Se pretende, asimismo, proporcionar los instrumentos teóricos indispensables para que sepa identificar las conductas que pueden ser constitutivas de infracciones administrativas o penales, a fin de que, si dichas acciones tienen por objeto los sistemas que administra, pueda detectarlas y denunciarlas.

Por ejemplo, es muy probable que a un profesional informático se le planteen numerosos interrogantes en el desempeño de su trabajo. Así, a un administrador de sistemas pueden surgirle las siguientes dudas:

- Si el jefe de la empresa me pide que acceda y le muestre el contenido del buzón de mensajes personales de un trabajador, ¿tengo la obligación de hacerlo?

- El servidor almacena datos de carácter personal y, por tanto, he de adoptar la implementación de medidas de seguridad determinadas. Si no lo hago, ¿incurro en algún tipo de responsabilidad?

- ¿Es posible el empleo de instrumentos criptográficos para proteger la información?

- ¿Es legal la utilización de escáneres, entendidos como instrumentos de administración de sistemas?

- Si se produce un acceso no autorizado al servidor y los intrusos modifican la página web de mi departamento, ¿se ha cometido algún delito? ¿Es un hecho denunciable? ¿Ante quién?

- ¿Cuáles son los actos que, en el contexto de los sistemas informáticos, debieran ser reprochados penalmente o sancionados con penas privativas de libertad?

- ¿Todo atentado contra el hard o el soft debe ser constitutivo de delito en sede penal?

- ¿Cuáles son los bienes jurídicos afectados por dichas conductas, esto es, aquellos valores relevantes para las personas y la sociedad toda –como la

vida, el patrimonio– que dada su importancia deben ser protegidos ante los delitos informáticos?

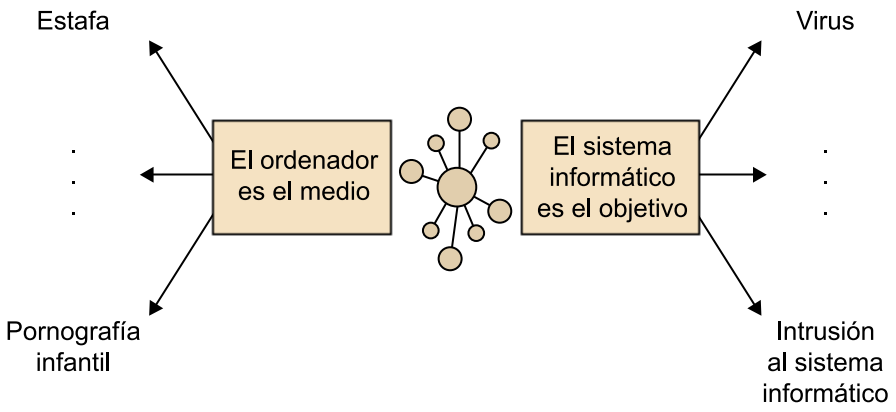
En este módulo intentaremos exponer las cuestiones esenciales que permitan solventar el mayor número posible de los interrogantes que se suscitan.

En primer lugar, recordaremos los distintos tipos de respuesta que el derecho ofrece ante este tipo de incidentes informáticos. Como sabéis, el incumplimiento de las normas da lugar a la imposición de sanciones, que pueden ser más o menos graves. Pues bien, deberemos tener en cuenta ambos tipos de respuesta (de carácter administrativo y de carácter penal), puesto que prevén sanciones de distinta gravedad.

Una vez esclarecido lo anterior, nos ceñiremos, en este módulo, al ordenamiento sancionador de carácter penal. Sin embargo, no se llevará a cabo un examen exhaustivo y detallado del Código penal ni de las sentencias relacionadas con los delitos vinculados a la criminalidad informática, sino que se ofrecerá una perspectiva general sobre las conductas punibles en el ordenamiento penal español. Para ello, será necesario abordar una primera cuestión, cifrada en la necesidad de distinguir los diversos tipos de contenidos o comunicaciones –ilícitas y nocivas–, que circulan por las redes de información, puesto que sólo serán delito las primeras de ellas.

Por último, se expondrán las generalidades de los delitos vinculados a la informática que contiene el Código penal español.

Delincuencia informática



Objetivos

Los materiales didácticos de este módulo proporcionan los contenidos y herramientas imprescindibles para alcanzar los siguientes objetivos:

1. Ofrecer una perspectiva general acerca de qué conductas resultan punibles en el ordenamiento penal español.

2. Distinguir los hechos lícitos de los ilícitos.

3. Advertir la diferente gravedad que pueden revestir los distintos delitos vinculados a la informática.

4. Detectar la posible comisión de delitos.

5. Analizar el marco legal y tomar decisiones ante posibles hechos ilícitos.

1. Prevención y sanción de delitos vinculados a Internet

Ved también

Podéis consultar al respecto los módulos "Protección de datos e intimidad" y "Los servicios de la sociedad de la información".

Las redes de comunicación electrónica y los sistemas de información forman parte de la vida diaria y desempeñan un papel fundamental en el crecimiento económico. Los sistemas de información y las redes están cada vez más interconectados y la convergencia es mayor. Por ello, se ha hecho necesaria la aprobación de algunas normas, que regulan varios aspectos –los más novedosos o los que no encuentran resolución aplicando las reglas generales– de la denominada sociedad de la información.

Sin embargo, Internet también es susceptible de usos abusivos o ilícitos, de forma que su generalizada implantación conlleva la aparición de nuevos riesgos y ataques.

Generalmente, al analizar la delincuencia vinculada a la informática, se han descrito dos categorías principales de riesgos.

1) En primer lugar, las amenazas a través del ordenador, es decir, delitos como la estafa, el blanqueo de dinero, la pornografía infantil, la violación de derechos de propiedad intelectual o el tráfico de drogas, realizados gracias al ordenador. Se trata de **figuras delictivas previstas tradicionalmente en los códigos penales, que revisten, ahora, una nueva forma de materializarse**.

2) En segundo lugar, los riesgos que pesan sobre las propias infraestructuras informáticas cuando son atacadas con el objetivo de alterar o impedir el normal funcionamiento de los sistemas de información. Así, por ejemplo, el acceso no autorizado a un ordenador o a una red de ordenadores; la difusión de programas informáticos perjudiciales –en sus múltiples modalidades de virus, bombas lógicas, caballos de troya, gusanos; ataques intencionados de denegación de servicio (DoS), que perturban o impiden los servicios ofrecidos por Internet y causan daños a las empresas que cuentan con un portal propio, desde el cual realizan operaciones con sus clientes, entre otros. En este caso, se trata de **nuevas figuras delictivas, que se están incorporando a los códigos penales**.

Pensad que estos ataques pueden lanzarse desde cualquier lugar del mundo hacia el resto y, además, en cualquier momento.

Algunas estadísticas resultan especialmente significativas:

1) De acuerdo con el Internet Complaint Center, durante su primer año de funcionamiento (2000-2001), recibió 30.503 quejas sobre fraudes en Internet.

2) De acuerdo con la Computer Crime and Security Survey del 2001, 186 empresas y agencias gubernamentales informaron de unas pérdidas económicas de más de 3,5 millones de dólares, debido principalmente al robo de información privada y al fraude financiero.

3) De acuerdo con Cabersnitch Voluntary Online Crime Reporting System, los crímenes relacionados con Internet abarcan desde la falsificación a la pornografía infantil, incluyendo el acoso en línea y las amenazas terroristas.

4) De acuerdo con Meridien Research, el coste del fraude en Internet alcanzó entre 5 y 15 millones de dólares en el 2005.

Foro

En el foro, se añadirán webs donde consultar estadísticas sobre los diversos ilícitos del año en curso o del anterior.

Ciberestadísticas. Expansión de la población con conexión

Nue Internet Surveys ha indicado que en febrero del 2002 había aproximadamente 544 millones de personas con conexión en todo el mundo. A medida que la población mundial aumenta su conexión, crecen también el número de potenciales sujetos activos del delito (autores) y de sujetos pasivos del mismo (víctimas).

Este creciente número de incidentes ha generado numerosas incertidumbres jurídicas en aquellos operadores o grupos de personas, que, de distinta forma, deben enfrentarse a este nuevo fenómeno y que básicamente se reducen a dos.

1) Los **profesionales de las tecnologías de la información**, que son a menudo los responsables de la primera línea de defensa y de descubrir los delitos (o ciberdelitos) cuando ocurren.

2) Los **profesionales vinculados a la Administración de justicia**, que son los que se encargan de investigar y perseguir dichos ilícitos.

Precisamente, para poder profundizar en el estudio de los ilícitos vinculados a la informática, empezaremos por diferenciar los distintos tipos de responsabilidad que pueden generar.

2. Responsabilidad administrativa y responsabilidad penal

La comisión de infracciones o conductas ilícitas vinculadas a datos personales engendra responsabilidad jurídica en dos sectores del ordenamiento jurídico de distinta gravedad: el orden administrativo (LOPDP) y el orden penal (Código penal).

Penas

Las sanciones previstas por el Código penal consisten, en gran parte de los casos, en penas privativas de libertad. Algunas de dichas penas suponen el ingreso en prisión.

La LOPDP contiene un **régimen jurídico sancionador administrativo** menos grave que el penal.

El artículo 43 LOPDP establece que los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador previsto en la ley. Por tanto, como se observa, la responsabilidad jurídica en este ámbito no es, necesariamente, de tipo personal, sino que puede recaer en una persona jurídica o empresa[1].

(1)Recordad que las figuras de responsable del fichero, encargado del tratamiento y responsable de seguridad pueden recaer en una persona jurídica o empresa.

El catálogo de **infracciones administrativas** previstas en la LOPDP se halla profusamente regulado en el art. 44 de la ley. Básicamente, se recogen tres tipos distintos de infracciones, que reciben la denominación de **leves, graves y muy graves**.

Así, por ejemplo, en ese exhaustivo elenco de conductas constitutivas de ilícito administrativo, se halla recogido **el incumplimiento de las medidas de seguridad** establecidas reglamentariamente [art. 44.2 h)], que en concreto **es considerado por la LOPDP** como una **infracción de carácter grave**.

Por tanto, en el supuesto en que el servidor almacene datos de carácter personal (como, por ejemplo, las direcciones IP), surge la obligación de notificar e inscribir el fichero ante la Agencia de Protección de Datos, así como de adoptar las medidas de seguridad que sean necesarias, en función del tipo de datos de que se trate (nivel básico, medio o alto).

La comisión de una infracción administrativa dará lugar a la aplicación de una sanción y, en caso de infracciones muy graves, puede permitir, también, la adopción de una medida accesoria o cautelar.

El cuadro sancionador se halla recogido en el artículo 45 LOPDP. Las sanciones consisten en una multa cuya cuantía dependerá de la gravedad de la infracción cometida.

Básicamente, el marco de la multa oscilará entre una cuantía mínima de 601 euros a una máxima de 601.012 euros, en función de la gravedad de la infracción (leve, grave o muy grave).

Además, la LOPDP, en su artículo 49, permite que en los supuestos de utilización o cesión ilícita de los datos, que son constitutivos de infracción muy grave, el director de la Agencia de Protección de Datos, además de ejercer la potestad sancionadora, requiera a los responsables de los ficheros la cesación en la utilización o cesión ilícita de los datos. Y si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros.

Ved también

Podéis consultar el apartado 20 del módulo "Protección de datos e intimidad" para repasar las infracciones y sanciones de la LOPDP.

3. Necesidad de distinción de contenidos en Internet

Internet, al igual que cualquier otra tecnología de la información, puede utilizarse como vehículo de actividades criminales o bien transmitir contenidos potencialmente ilícitos o nocivos.

En principio, dichas conductas están sujetas al marco jurídico actual, es decir, a las legislaciones estatales respectivas.

Ahora bien, para poder analizar posteriormente la posible determinación de responsabilidades, resulta conveniente abordar la diferencia entre contenido ilícito y contenido nocivo:

1) Los contenidos dañosos o nocivos dependen de diferencias culturales y reclaman la idea de generar una cultura ética o deontológica en Internet, que, respetando las diversidades culturales, responda a unos mínimos estándar. En este contexto de protección frente a posibles materiales ofensivos, se han de respetar plenamente los derechos fundamentales y, especialmente, el derecho a la libertad de expresión.

2) Los contenidos ilícitos representan comportamientos atentatorios de derechos y, por eso, suelen estar previstos como delictivos por las legislaciones internas de los países.

Esa diferencia resulta trascendental, puesto que desencadena respuestas distintas.

1) Es decir, sólo los **contenidos ilícitos** deben ser combatidos –y, por tanto, controlados– por los poderes públicos, es decir, por el Estado.

2) En cambio, los **contenidos dañosos** reclaman, fundamentalmente, una intervención privada a cargo de los propios usuarios (software de filtrado, señales acústicas o visuales, etiquetas de advertencia), como se verifica en otros medios de comunicación analógicos. Es decir, las acciones frente al contenido nocivo deben, prioritariamente, intentar ofrecer a los usuarios soluciones tecnológicas (sistemas de filtrado y clasificación) para rechazar tales contenidos.

Así, por ejemplo, la iniciativa lanzada recientemente, en EE. UU., Canadá y México, por Yahoo!, AOL y Microsoft, mediante la instalación de unas etiquetas de advertencia, en aquellas web cuyo contenido pueda ser perjudicial o dañino para los menores.

También en el ámbito de la Unión Europea se ha subrayado que estas dos categorías de contenidos plantean cuestiones de principio radicalmente distintas y reclaman, por tanto, respuestas jurídicas y tecnológicas muy diversas.

Mientras que las medidas sobre contenidos ilícitos deberían dirigirse contra la fuente, los contenidos nocivos exigen medidas para aumentar la sensibilización y la capacitación de los usuarios.

Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Contenidos ilícitos y nocivos en Internet, de 16 de octubre de 1996, COM (96) 487 final; Libro Verde *La protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información*, de 16 de octubre de 1996, COM (96) 483 final e Informe provisional sobre las iniciativas emprendidas en los Estados miembros de la Unión Europea contra los contenidos ilícitos y nocivos en Internet, de 4 de junio de 1997 (versión 7).

El Plan de acción para promover una utilización segura de Internet establece que el contenido ilegal debe ser tratado en su origen por las autoridades de policía y las judiciales, cuyas actividades están protegidas por las leyes nacionales y por los acuerdos de cooperación judicial.

Referencia bibliográfica

Comunicación de la Comisión al Parlamento Europeo y al Consejo. Plan de Acción para la Promoción del Uso Seguro de Internet, de 26 de noviembre de 1997, COM (97) 582 final.

Según el Plan de la Comisión, el contenido ilegal abarca una gran variedad de problemas, entre los que destacan los siguientes:

1) Seguridad nacional (instrucciones sobre la confección de bombas, producción de drogas ilegales, actividades de terrorismo).

2) Protección de los menores (formas abusivas de marketing, violencia, pornografía).

3) Protección de la dignidad humana (incitación al odio racial, discriminación racial).

4) Seguridad económica (fraude, instrucciones para piratear tarjetas de crédito).

5) Protección de la información (acceso ilegal y malévolo).

6) Protección de la vida privada (comunicación no autorizada de datos de carácter personal, hostigamiento electrónico).

7) Protección de la reputación (calumnia, publicidad comparativa ilegal).

8) Propiedad intelectual (difusión no autorizada de obra protegida por derechos de autor).

Por tanto, podemos concluir que **sólo las comunicaciones con contenido ilícito pueden generar responsabilidad penal**.

4. La errónea noción de delito informático

Los ilícitos perpetrables a través de Internet no son reconducibles a una categoría única y homogénea. Los ilícitos vinculados a la informática pueden lesionar bienes jurídicos diversos. De ahí que sea incorrecto hablar del delito informático como si todos los incidentes de la red vulnerasen el mismo valor o bien jurídico. De hecho en el Código penal no aparece previsto el delito informático como tal categoría.

En este sentido, parece preferible hacer referencia a este tipo de delito como **delitos vinculados a la informática** o **conductas relativas a la criminalidad informática**.

El objetivo de este módulo es dar a conocer a los administradores de un sistema informático las responsabilidades en las que pueden incurrir a causa de su trabajo y, como punto principal, dotarlos de mecanismos que, en el caso de acciones delictivas que tienen por objeto los sistemas que administran, les permitan denunciar los delitos de los que han sido víctimas y solicitar las actuaciones legales pertinentes.

Por otro lado, tampoco se pretende elaborar una recopilación excesivamente generosa en lenguaje jurídico, ni profundizar en posibles sentencias relacionadas con los delitos que se explicarán en este capítulo. La legislación actual todavía presenta vacíos con respecto a los mal llamados delitos informáticos, de manera que se ofrecerán directrices básicas relativas con el Código penal.

La vertiente tecnológica o científica de los estudios de ingeniería a menudo roza la parte social de la aplicación de los avances que se van produciendo en estas disciplinas. En consecuencia, el administrador de un sistema puede ser muy competente en el trabajo técnico, pero es posible que albergue muchas dudas cuando se enfrenta a problemas como los siguientes:

1) Si mi jefe me pide que le muestre el contenido del buzón de correo personal de un trabajador, ¿tengo la obligación de hacerlo?

2) Se ha producido un acceso no autorizado en el servidor y los intrusos han modificado la página web del departamento. ¿Este hecho es denunciable? ¿A quién lo debo denunciar?

3) ¿Es legal la utilización de escáneres (entendidos como herramientas de administración de sistemas)?

4) ¿Puedo utilizar herramientas criptográficas para proteger la información?

En el siguiente apartado intentaremos orientar al administrador en relación con las dudas que se han expresado, si bien es necesario ser consciente de que no existe una línea de actuación única, y las particularidades de cada caso provocan que se deba ser muy prudente a la hora de enfrentarse con este tipo de problemas.

5. Delitos vinculados a la criminalidad informática en el Código penal español

La proliferación y diversidad de formas que pueden adoptar los ataques contra los sistemas de información constituye una de las características de la ciber-criminalidad.

A los efectos que interesan, estudiaremos los siguientes:

1) Delitos contra la intimidad (arts. 197 a 200 CP)

2) Delito de fraude informático (art. 248.2 CP)

3) Delito de utilización abusiva de equipos (art. 256 CP)

4) Delito de daños informáticos (art. 264 CP)

5) Delitos contra la propiedad intelectual (art. 270 CP)

6) Delitos contra los secretos de empresa (art. 278.1 CP)

7) Delitos contra los intereses económicos de los prestadores de servicios (art. 286 CP)

8) Delitos de pornografía infantil (art. 189 CP)

9) Otros ilícitos penales

10) Las conductas de *hacking* o de accesos inconsentidos a los sistemas

El estudio pormenorizado de todos estos delitos excede los objetivos prefijados en estos materiales. Por tanto, su análisis será necesariamente breve.

5.1. Delitos contra la intimidad (arts. 197 a 200 CP)

Derecho a la intimidad

La Constitución española reconoce el derecho a la intimidad en el artículo 18.

El artículo 197.1 del vigente Código penal (en adelante, CP) ha incorporado acertadamente los avances tecnológicos que tantos riesgos generan para la privacidad informática.

Así, se equiparan conductas como la interceptación de correo electrónico con la violación de correspondencia.

En concreto, a tenor de lo previsto en el artículo 197.1 CP, son comportamientos constitutivos de delito:

- El apoderamiento de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales.
- La interceptación de las telecomunicaciones.
- La utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier o otra señal de comunicación.

El Código penal exige que dichas conductas[2] se lleven a cabo con la concurrencia de **dos requisitos**:

[(2)]Las conductas de *sniffing*, por tanto, tendrían perfecto encaje en este precepto.

a) que sean **sin consentimiento** del afectado;

b) que se lleven a cabo **con la intención de descubrir los secretos o vulnerar la intimidad ajena**.

Este último requisito (exigencia del ánimo de descubrir la intimidad ajena) resulta especialmente problemático en el ámbito probatorio.

Al respecto, resultan ilustrativos

1) El **Caso Hispahack** (Sentencia de 28.5.1999, del Juzgado de Instrucción núm. 2 de Barcelona)

2) y el **Caso Ministerio del Interior** (Auto de 29.1.2002, del Juzgado de Instrucción número núm. 2 de Lorca).

Por tanto, si retomamos algunos de los interrogantes planteados al comienzo del epígrafe, ya podemos afirmar que, como regla general, **acceder a los mensajes de correo electrónico ajenos puede ser constitutivo de delito**.

5.1.1. Interceptación del correo electrónico del trabajador

Dada la generalizada implantación de las nuevas tecnologías en el ámbito laboral, la discusión sobre si la vigilancia o monitorización de la actividad del trabajador y, más concretamente, la interceptación del correo electrónico de los trabajadores puede llevarse a cabo de forma lícita o, por el contrario, resulta constitutiva de delito, constituye una cuestión controvertida.

La cuestión relativa a la licitud de la conducta de monitorizar o interceptar las comunicaciones ajenas supone un conflicto jurídico entre dos derechos. De una parte, el derecho a la intimidad del trabajador y de otra, las facultades de

supervisión y control que el Estatuto de los trabajadores (artículo 20.3) otorga al empresario para que se asegure de que el trabajador cumple adecuadamente con sus obligaciones.

En principio, deben diferenciarse adecuadamente las diversas medidas que puede adoptar el empresario. Es decir, hay que distinguir aquellos casos en que se lesiona el derecho al secreto de las comunicaciones (por ejemplo, porque se accede al correo electrónico) de las medidas que inciden en el derecho a la intimidad (monitorización de la actividad, lectura de cabeceras, asunto, etc.).

La conducta de acceso al correo electrónico es la más grave y en la mayor parte de los casos constituye una conducta ilícita. Por el contrario, el resto de medidas suponen una intromisión de menor gravedad. Al respecto, pueden sugerirse algunas reflexiones generales para que estas medidas se produzcan sin vulneración de su intimidad.

En primer lugar, sería deseable que ese control estuviese previsto en la normativa interna de la organización empresarial.

Artículo 197

El uso de herramientas de monitorización de la actividad de un sistema en el terminal de un trabajador (sin su consentimiento) también podría incluirse dentro del artículo 197.

En segundo lugar, que se haya pactado con los sindicatos y que, por tanto, los trabajadores tengan conocimiento de que pueden ser objeto de dicha medida de control.

Por último, el acceso al correo electrónico sólo podrá llevarse a cabo ante sospechas fundamentadas de incumplimientos graves por parte de los trabajadores (espionaje empresarial, acoso sexual, envío de virus, etc.). Aun así, el acceso debe perseguir una finalidad específica, explícita y legítima, debe tratarse de una respuesta proporcionada y debe suponer el mínimo impacto para la intimidad del trabajador. Es decir, si es posible, el conflicto debe solventarse con otras medidas menos lesivas de la intimidad, como, por ejemplo, el bloqueo del correo, la lectura de la cabecera, del flujo o del número de bites, entre otras.

Tener en cuenta los requisitos que he mencionado antes (distinción del derecho afectado, sospechas fundadas de incumplimientos graves, con una finalidad específica, explícita y concreta, proporcionalidad de la respuesta) es fundamental. Si el empresario sospecha que el trabajador incumple, siempre debe acudir al medio menos lesivo para la intimidad del trabajador. Por ejemplo, la cabecera de los correos, el tráfico generado, etc. Y si cree que es delictivo, debe denunciar.

Por otra parte, recientemente el Tribunal Supremo ha dictado una sentencia (Sentencia de 26 de septiembre del 2007) (Sala de lo Social, es decir, no Sala de lo Penal), en un intento de unificar doctrina, que aporta algo importante. Básicamente, dice que es necesario que el empresario proponga una política uniforme y razonable de usos de las NTC de la empresa (consensuadas con

sindicatos) y que se haga saber a los trabajadores dicha política. Y si esto se cumple, en cierta forma, se amplían las facultades del empresario para fiscalizar el uso de dichas herramientas.

En resumen, no resulta aceptable que la interceptación pueda ser llevada a cabo aleatoriamente como medida de control, porque supone una indiscutible vulneración de la intimidad del trabajador y, por tanto, resulta una conducta delictiva castigada en el art. 197.1 CP.

El Código penal español contiene, también, un régimen sancionador de algunas conductas vinculadas a lo que se suele denominar **abusos informáticos** sobre datos personales. En este caso, **la responsabilidad jurídica es de orden penal y, por tanto, de carácter estrictamente personal**.

Es decir, la responsabilidad derivada de la comisión de alguno de esos delitos o ilícitos penales sólo podrá recaer en personas físicas, pero nunca en personas jurídicas o entidades.

El cuadro normativo previsto en el Código penal es muy amplio. No obstante, conviene especialmente abordar dos modalidades concretas de ilícitos, previstas en los arts. 197.2 y 199.2 CP, respectivamente.

1) El artículo 197.2 del Código penal castiga las conductas de **acceso, utilización o modificación de datos personales, llevadas a cabo sin autorización, esto es, con ausencia de autorización legal**.

A su vez, sobre la conducta descrita el código construye figuras agravadas, que suponen un incremento de la pena. A los efectos que aquí interesan, merece la pena destacar las siguientes **modalidades agravadas**:

1) El código castiga (art. 197.4, primer inciso) la conducta de quienes, **tras haber llevado a cabo el acceso**, modificación o utilización ilícita de los datos, **revelan o ceden ilícitamente a terceros** esos datos descubiertos o modificados.

2) Asimismo, el Código penal castiga (art. 197. 5, primer inciso) la conducta anteriormente descrita cuando es llevada a cabo, precisamente, por **el responsable del fichero o el encargado del tratamiento**. Si, posteriormente, además se ceden o revelan ilícitamente los datos, el Código obliga al juzgador a imponer la pena en su mitad superior.

3) El Código también incrementa la pena si las conductas anteriormente descritas tienen por objeto **datos personales especialmente sensibles**, esto es, aquellos que conforman el denominado núcleo duro de la intimidad, a saber, datos relativos a la ideología, religión, creencias, salud, origen racial o vida sexual.

4) Por último, si los hechos descritos se llevan a cabo con **fines lucrativos**, el Código prevé que las penas que llevan aparejadas cada uno de los delitos señalados se impongan siempre en su mitad superior.

2) El segundo precepto penal particularmente interesante en materia de abusos informáticos sobre datos personales es el artículo 199.2 del Código penal.

Este delito castiga la conducta del profesional que, con incumplimiento de su obligación de sigilo o reserva, divulga los secretos de otra persona, con pena de prisión e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

En la interpretación y posible aplicación de este precepto debe recordarse que la LOPDP instituye un deber de secreto a cargo de quienes participan en el tratamiento de datos personales.

El art. 10 LOPDP establece que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos.

5.2. Delito de fraude informático (art. 248.2 CP)

El art. 248.2 a) CP castiga a quien valiéndose de alguna **manipulación informática o artificio semejante consiga la transferencia no consentida de cualquier activo patrimonial**, con ánimo de lucro y perjuicio para tercero.

Los **requisitos** exigidos son:

- Que el autor actúe movido por el **ánimo de lucrarse**.
- Que el autor **quiera perjudicar al tercero** sobre cuyo patrimonio lleva a cabo la manipulación informática.

En la actualidad, los casos de fraude informático más frecuentes son:

1) Casos de *phishing*: se obtiene información económica y datos personales (contraseñas), mediante correos con direcciones falsificadas y duplicación ilícita de páginas webs. En Reino Unido: Barclays, LLoydsTSB y Natwest; sitio de subastas online eBay. Éxito: 1-20. En España: Caja Madrid.

2) Casos de *pharming*: el usuario cree estar accediendo a un sitio web mientras que, en realidad, está accediendo a otro (mapeo de IP de una dirección a otra).

A finales del 2003 se aprobó la Ley 15/2003 (en vigor desde el 1 de octubre del 2004), que supuso una profunda reforma del Código penal español en algunos de los delitos vinculados a la criminalidad informática.

Concretamente, en materia de estafa informática, se introdujo un nuevo apartado (art. 248.2 b) CP), por el que se incorpora el castigo de conductas preparatorias para la comisión de estafas o fraudes informáticos.

Así, se castiga la fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados a la comisión de las estafas de los párrafos anteriores.

El castigo de estos actos preparatorios para la comisión de un delito ya se prevé en otros ámbitos del Código (delitos contra la propiedad intelectual, falsedades y delitos contra los prestadores de servicios).

Por último, la LO 5/2010, de 22 de junio, por la que se modifica el Código penal, ha incorporado una nueva modalidad de estafa:

Se castiga la **utilización de tarjetas de crédito o débito**, o cheques de viaje, o los datos obrantes en cualquiera de ellos, **para realizar operaciones de cualquier clase en perjuicio de su titular o de un tercero**.

¿Sabíais que....?

Con la introducción de la estafa informática, se logra superar uno de los inconvenientes legales que no permitían castigar este tipo de fraudes con anterioridad al CP de 1995. La figura delictiva de la estafa exige una relación psicológica de engaño entre autor y víctima. Este requisito se ha sustituido, en la estafa informática, por el de la **manipulación informática o artificio semejante**.

Reflexión

Reflexionad en el foro sobre la conveniencia o la necesidad de castigar la tenencia de esos instrumentos en los delitos mencionados (estafas, propiedad intelectual, falsedades, etc.).

5.3. Delito de utilización abusiva de equipos (art. 256 CP)

El art. 256 CP castiga el **uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular**, ocasionando a éste un perjuicio superior a 400 euros.

Los **requisitos** exigidos por el Código son:

- la producción de perjuicio evaluable económicamente,
- la afección al titular del equipo y no a tercero.

5.4. Delito de daños informáticos (art. 264 CP)

Las conductas de daños informáticos se concretan en asaltos sobre máquinas o sistemas informáticos para ocasionar perturbaciones sobre dichos sistemas o para modificar o destruir datos.

Esto es, se trata de comportamientos llevados a cabo **con el ánimo de perturbar los sistemas informáticos o de destruir los datos** que contienen.

Una de las acciones más peligrosas radica en el acceso inconsentido a los sistemas informáticos, con el fin de implementar un virus que produzca los resultados anteriormente indicados.

Actualmente, se ha constatado el aumento en la creación, divulgación e infección a causa de virus informáticos, así como de los cuantiosos daños económicos provocados por éstos. Son también frecuentes los asaltos a los encaminadores (*routers*), desde los que lanzar ataques masivos de denegación de servicio (DOS) (*smurfing*).

Daños económicos de los virus

Los virus informáticos han causado importantes daños económicos. Así, por ejemplo, en el 2001, Nimda provocó pérdidas de 630 millones de dólares, Code Red, de 2.620 millones, SirCam, de 1.150; en el 2000 I love You, de 8.750 millones y, en 1999, Melissa causó pérdidas de 1.100 millones y Explorer de 1.020 millones de dólares.

En este ámbito delictivo, la reforma del Código penal del 2010 también ha supuesto novedades significativas.

1) Con carácter previo a la reforma, el art. 264.2 CP castigaba la **destrucción, alteración, inutilización u otro daño de los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos**.

Los mayores **problemas** que planteaba la aplicación de este delito se referían a los siguientes aspectos:

a) La exigencia de perjuicio económico, cifrado en 400 euros. La valoración económica de los perjuicios generados por los daños no es un proceso sencillo y, en algunas ocasiones, no es posible llevarlo a cabo de modo inmediato.

b) Limitación del objeto sobre el que recae la acción a los datos, programas o documentos electrónicos, sin que se haga referencia al funcionamiento de los sistemas. Se trataba de un problema relativo, puesto que los incidentes sobre los sistemas se llevan a cabo implementando virus y éstos modifican los ejecutables a los que contaminan (alteran datos).

2) La LO 5/2010, de modificación del CP, ha seguido las directrices establecidas en la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero del 2005, relativa a los ataques contra los sistemas de información, aprobada por la Unión Europea. Esta Decisión Marco se encarga de regular las conductas de acceso no consentido a un sistema informático y las conductas de intromisión ilegal en los sistemas de información y en los datos.

En este sentido, la reforma ha incorporado la regulación prevista en la norma de la Unión Europea y el nuevo art. 264 establece lo siguiente:

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

b) Quien por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

Esta nueva configuración de los daños informáticos presenta novedades importantes respecto de la anterior.

1) Se ha producido una ampliación del objeto sobre el que recae la conducta, que puede ser los datos, programas informáticos o documentos electrónicos y los sistemas informáticos.

2) Se han separado adecuadamente las conductas que inciden sobre los datos y las que afectan a los sistemas.

3) El delito de daños informáticos deja de ser una modalidad dependiente del delito de daños en cosa material y, por tanto, **desaparece la exigencia del perjuicio económico cifrado en 400 euros** (que sí se exige en el delito de daños en cosa material). Así, con la nueva redacción, lo que deberá tenerse en

cuenta es el daño funcional, para cuyo cómputo podrá tenerse en cuenta el valor en sí de los datos, su utilidad y el reflejo de tal pérdida en la utilización del titular de los datos.

4) Se exige que la conducta se lleve a cabo de manera grave y que el resultado sea también grave, aunque en ningún momento se concretan los criterios de gravedad. Ello podría plantear problemas a la hora de delimitar aquellos ataques molestos pero no suficientes como para motivar la intervención penal de aquellos otros que, por su mayor gravedad, sí merecen reproche penal.

Para que se cometa el delito, es decir, para que el envío o la implementación de un virus sea una conducta delictiva, es necesario que el autor lleve a cabo la conducta con la **voluntad de causar el daño**.

5.5. Delitos contra la propiedad intelectual (art. 270 CP)

En estos delitos, interesa destacar **tres** modalidades delictivas:

1) El art. 270.1 castiga **la reproducción, distribución o comunicación pública, en todo o en parte, de una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, con ánimo de lucro y en perjuicio de tercero**.

Como ya se ha expuesto anteriormente (al analizar la ley de propiedad intelectual), en la protección de la propiedad intelectual es irrelevante el soporte en el que se plasme la obra, es decir, puede tratarse de textos, programas de ordenador, vídeos, canciones, gráficos, entre otros.

Por tanto, las conductas de reproducción, distribución o comunicación pública de cualquiera de los objetos mencionados constituyen un delito contra la propiedad intelectual.

El artículo 270 CP requiere la concurrencia de dos elementos para que la conducta pueda ser considerada delictiva:

a) El ánimo de lucro
b) El perjuicio de tercero

Uno de los requisitos más importantes que exige este precepto es el relativo al ánimo de lucro.

Ese elemento implica que, para que la conducta pueda ser perseguida, es necesario probar que el autor reproduce, distribuye o comunica la obra **con ánimo de enriquecerse ilícitamente**.

Precisamente, ése elemento es el que, hasta ahora, ha motivado que:

a) La mayor parte de procesos penales por conductas de reproducción y distribución de contenidos a través de plataformas P2P acaben en absolución.

Sentencias

Así, podéis consultar la sentencia del Juzgado de lo Penal núm. 3 de Santander, de 14 de julio del 2006 o la sentencia del Juzgado de Instrucción núm. 1 de Madrid, de 19 de marzo del 2008, ambas absolutorias en procesos dirigidos contra usuarios de P2P.

b) También, ese elemento es el que ha generado resoluciones contradictorias en cuanto al fenómeno top-manta.

Algunos tribunales absuelven a los que distribuyen obras, sin autorización de los titulares de los derechos, en la vía pública. En esas resoluciones, se insiste en que los autores, generalmente inmigrantes con escasos recursos económicos, representan sólo el último eslabón de una cadena comercial controlada y dirigida por mafias criminales. De ahí que apliquen el principio de proporcionalidad, de intervención mínima o de insignificancia y, en consecuencia, absuelvan.

Sin embargo, este ámbito (relativo al top-manta o a la distribución callejera de obras a bajo precio) también se ha visto modificado por la reforma del 2010.

2) La reforma ha introducido un párrafo segundo al apartado 1 del art. 270 CP, con la siguiente redacción:

> No obstante, **en los casos de distribución al por menor, atendidas las características del culpable y la reducida cuantía del beneficio económico**, siempre que no concurra ninguna de las circunstancias del artículo siguiente, el Juez podrá imponer la pena de multa de tres a seis meses o trabajos en beneficio de la comunidad de 31 a 60 días. En los mismos supuestos, cuando el beneficio no exceda de 400 euros, se castigará el hecho como falta del artículo.

La introducción de este nuevo apartado permite la aplicación del Código penal aunque no concurran los elementos anteriormente expuestos y, en especial, el ánimo de lucro. Por tanto, esta nueva previsión conllevará una ampliación de la intervención penal en supuestos de venta callejera. La eliminación de esos elementos típicos, presentes en el art. 270.1 CP, dificultará a ciertos tribunales proseguir en esa tendencia absolutoria.

Se trata de una reforma censurable puesto que existen otras vías menos severas (administrativa y, en su caso, civil) para responder al fenómeno del top-manta. Por otra parte, la pena de multa no parece necesaria ni útil dadas las características del autor de este tipo de distribución, a saber, inmigrantes sin recursos económicos que encarnan el último eslabón de la cadena comercial.

3) El art. 270.3 castiga **la fabricación, importación, puesta en circulación y tenencia de medios destinados específicamente destinados a facilitar la supresión no autorizada o la neutralización de los dispositivos técnicos utilizados para proteger programas de ordenador o cualquiera de las otras obras**.

De esta modalidad, interesa que reflexionéis sobre dos cuestiones:

a) Se otorga, así, una tutela ya reclamada por la Directiva 91/250, de 14 de mayo, adoptada por el Consejo de las Comunidades Europeas, sobre protección de programas de ordenador, instando a los Estados miembros a adoptar las disposiciones de derecho interno necesarias para su cumplimiento.

> **Concretamente, el artículo 7 de la directiva establece que los Estados miembros**, de conformidad con sus legislaciones nacionales, deben adoptar medidas oportunas para evitar la puesta en circulación de una copia de un programa de ordenador conociendo su origen ilícito, la tenencia con fines comerciales de una copia de un programa de ordenador conociendo o pudiendo suponer su naturaleza ilegítima, así como la puesta en circulación o tenencia con fines comerciales de cualquier medio apto para facilitar la supresión o neutralización de cualquier dispositivo técnico utilizado para la protección de un programa de ordenador.

Además, ante la presión de la industria musical y cinematográfica, la reforma del 2003 amplió el objeto de tutela. Antes de dicha reforma, sólo se protegían los programas de ordenador; tras la Ley 15/2003, se añade la protección de **cualquiera de las otras obras**.

b) Se castiga la fabricación, distribución o tenencia de dispositivos o instrumentos técnicos para defraudar los derechos de autor.

Por tanto, al igual que ocurría en la estafa informática, se está **adelantando el castigo a los actos preparatorios para cometer un delito**.

Fijaos que lo que se sanciona es el uso de herramientas lógicas (software de grabación) o aparatos de grabación que vulneren la protección que algunos soportes (CD, DVD) incluyen, para hacer copias privadas.

A nuestro juicio, y teniendo en cuenta que una vez vendido (software, grabadoras), el fabricante no puede controlar el uso que de él hace el usuario (magnetoscopio de Sony), será una conducta punible si dichos dispositivos son **susceptibles sólo de uso ilícito: medios específicamente destinados. Pero no en el resto de casos, esto es, cuando el dispositivo también es susceptible de usos lícitos**.

Las conductas de *cracking*, con arreglo a su significación originaria, se caracterizan por eliminar o neutralizar los sistemas de protección de un sistema informático, ya sea de un programa o del propio sistema operativo de la máquina.

Cracker

El término *cracker* fue acuñado en 1985 para diferenciar –y defender– estas conductas de las de los *hackers*, ante el mal uso periodístico de este último término. Esta tendencia a deslindar estos dos comportamientos se ha perpetuado, de modo que, actualmente, en algunas ocasiones, se suele acudir a las expresiones *de black hack* o *black hat*, como sinónimos de cracker, para distinguirlas de la conducta del *hacker*, al que también se hace referencia con las antónimas de *white hack* o *white hat*.

Habitualmente, se rompe la protección de un programa que impide su copia no autorizada o la de una aplicación *shareware* que impide su uso, pasada una determinada fecha. Este comportamiento se cifra, pues, en la copia inconsentida y, en su caso, posterior distribución ilegal, de programas informáticos (denominados *warez*, esto es, programas comerciales que han sido sometidos a la acción de un *crack*), con vulneración de los derechos de autor.

Lectura complementaria

D. Ferrandis Ciprián (2001). "Glosario" (pág. 175). En: E. Orts Berenguer; M. Roig Torres. *Delitos informáticos y delitos comunes cometidos a través de la informática*. Valencia: Tirant lo Blanch.

Así pues, **encontrarán respuesta penal** en el mencionado precepto, por ejemplo, **los siguientes comportamientos**:

1) La reproducción, total o parcial, de programas de ordenador.

2) La instalación de copias no autorizadas de programas de ordenador.

3) La publicación de códigos fuente de programas de ordenador, de programas diversos (servidores de *warez*), ficheros (MP3, texto) en Internet, sin el consentimiento del titular de los derechos de distribución.

4) La inutilización de mecanismos de protección que permiten el funcionamiento correcto del programa (mochilas, contraseñas y otros instrumentos de seguridad), es decir, conductas de *cracking*.

En el Código penal vigente hasta octubre del 2004, la persecución de estos delitos necesitaba la denuncia de la persona agraviada o de sus representantes legales, excepto si afectaba a los intereses generales o a una pluralidad de personas (art. 287 CP).

Sin embargo, desde la reforma introducida por la Ley15/2003, se puede actuar de oficio por parte de los cuerpos policiales.

5.6. Delitos contra los secretos de empresa (art. 278.1 CP)

El art. 278.1 CP castiga **la interceptación de cualquier tipo de telecomunicación o utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación**.

Este delito permite castigar el **espionaje empresarial informático**, esto es, el apoderamiento de información empresarial secreta que representa un valor económico para la empresa.

Pensad que esa información puede ser de cualquier tipo: industrial (invenciones, diseños.), comercial (listados de clientes, de proveedores) o referida al ámbito de la organización interna de la propia empresa (estrategias publicitarias, planes de inversión, condiciones que renegociar con un cliente).

Su aplicación requiere que la interceptación sea llevada a cabo **para descubrir un secreto de empresa**.

5.7. Delitos contra los intereses económicos de los prestadores de servicios (art. 286 CP)

La reforma del 2003 introdujo este novedoso precepto que incluye cuatro modalidades delictivas:

1) Se castiga la facilitación del acceso inteligible a servicios de radiodifusión sonora o televisiva o a servicios interactivos prestados a distancia por vía electrónica, mediante la **facilitación, importación, distribución, posesión de programas o equipos informáticos**, diseñados o adaptados para hacer posible dicho acceso y subsiguientes secuencias lógicas, esto es, la **instalación, mantenimiento o sustitución** de los mismos, **con fines comerciales**.

2) Se castiga la **alteración o duplicación del número identificativo de equipos de telecomunicaciones, con ánimo de lucro**.

3) Se castiga la **facilitación de dicho acceso**, o suministro de información a una pluralidad de personas por medio de una comunicación pública, comercial o no, sobre cómo conseguirlo, **sin ánimo de lucro**.

4) Se castiga la **utilización de dichos equipos o programas** que permitan el acceso **o** la **utilización de los equipos alterados**, con independencia de la cuantía de la defraudación.

5.8. Delitos vinculados a la pornografía infantil (art. 183 bis y 189 CP)

Los delitos relativos a la pornografía infantil constituyen uno de los ámbitos en los que se han producido mayores reformas en los últimos tiempos.

En general, todas estas modificaciones (incluidas las de la reforma de 2010) suponen un endurecimiento de las penas y la incriminación de conductas que, hasta ahora, eran impunes.

Los delitos contra la libertad sexual han sido objeto de una profunda reforma en los últimos años, a través de las Leyes 15/2003 y 5/2010.

El Código penal de 1995 castiga una serie de conductas como modalidades básicas y otros supuestos como modalidades agravadas, esto es, más graves y, por tanto, castigadas con penas más severas.

Vamos a empezar con las **modalidades** delictivas **básicas**.

Constituyen delitos las siguientes conductas:

1) Contactar con un menor de 13 años a través de Internet, el teléfono o cualquier otra tecnología de la información con la finalidad de concertar un encuentro para cometer algún delito contra la libertad sexual del menor (incluida la producción de pornografía) siempre que el autor realice algún acto dirigido a acercarse al menor: prisión de 1 a 3 años.

2) Captación y utilización de menores **con fines o en espectáculos pornográficos o exhibicionistas** o para **elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte o lucrarse con ello**: prisión 1 a 5 años. El consentimiento del menor es irrelevante.

3) Producción, venta, distribución, exhibición, ofrecimiento o facilitación de las anteriores conductas: prisión 1 a 5 años.

4) Posesión para los fines de producción, venta, distribución, exhibición, ofrecimiento o facilitación de las anteriores conductas, prisión 1 a 5 años.

5) Posesión para uso propio de material pornográfico, en cuya elaboración se hubieran utilizado menores de edad o incapaces: prisión de 3 meses a 1 año.

6) Hacer participar al menor en un comportamiento sexual que perjudique la evolución o desarrollo de la personalidad de éste: prisión de 6 meses a 1 año.

7) Se amplía la incriminación de conductas a la producción, venta, distribución, exhibición o facilitación por cualquier medio de material pornográfico, **en el que no hubieran sido utilizados directamente menores o incapaces, con empleo, no obstante, de su voz o imagen alterada o modificada**: por tanto, pornografía técnica y simulada.

Se incluyen como **modalidades agravadas**: castigadas con penas más **graves** (esto es, con prisión de 5 a 9 años) las comisión de las anteriores conductas si concurren las siguientes circunstancias:

1) Utilización de **menores de 13 años**.

2) Identificación en los hechos de **caracteres** particularmente **degradantes** o **vejatorios**.

3) Consideración de los hechos de especial gravedad en atención al **valor económico del material pornográfico**.

4) Tepresentación de niños o incapaces que son **víctimas de violencia física o sexual** en el material pornográfico (películas SNAFF).

5) Pertenencia a organización o asociación, dedicada a la realización de las actividades previstas en el tipo básico.

6) Concurrencia en el responsable del delito de la condición de **ascendiente, tutor, curador, guardador, maestro** o de persona encargada de hecho o de derecho del menor incapaz.

5.9. Otros ilícitos penales

Además de los delitos mencionados, se pueden cometer otros muchos ilícitos mediante las nuevas tecnologías. Así, por ejemplo, amenazas y coacciones (a través de chats, correo electrónico), falsedades documentales (alteraciones y simulaciones de documentos públicos o privados), entre otros.

5.10. Las conductas de *hacking* o de accesos inconsentidos a sistemas

5.10.1. Definición de la conducta de *hacking* (*white hacking*)

Las conductas de *hacking* constituyen un fenómeno controvertido de difícil definición. En derecho español se ha producido, recientemente, una reforma al objeto de incorporar al Código penal esas conductas. Según se explicará posteriormente, esa nueva regulación revela un entendimiento erróneo de estas conductas y su valoración no es, por tanto, positiva.

Así pues, a fin de que podáis comprender mejor la regulación vigente y la que entró en vigor a finales del 2010, empezaremos por hacer algunas consideraciones sobre dichas conductas.

Con la expresión *hacking* se hará referencia a conductas de acceso no autorizado a sistemas informáticos, desprovistas de cualquier intención distinta al acceso mismo.

En este sentido, debe tenerse en cuenta que el acceso no autorizado a un sistema puede llevarse a cabo con un ánimo inherente a lo que se describirá como la idiosincrasia del *hacker* y que responde, fundamentalmente, a un deseo de curiosidad y de reto constante frente a los sistemas informáticos, o bien puede obedecer a motivaciones ulteriores y más graves, como espiar, defraudar, sabotear, etc. En este último caso, al acometerse con una intención delictiva, no se corresponden estrictamente con la definición de *hacker*.

En estos casos (en los que hay una finalidad delictiva ulterior), el acceso no autorizado deviene *modus operandi* y queda absorbido por el hecho principal perseguido por el autor (es decir, el correspondiente delito contra la intimidad, de daños, de estafa, etc.).

No es correcto identificar la conducta del *hacker* con la del delincuente informático, con carácter genérico, puesto que las conductas de mero acceso (o de *hacking*) tienen una caracterización criminológica propia. Los accesos no autorizados del *hacker* responden a diversas motivaciones que pueden ser reconducidas a una insaciable curiosidad por los sistemas informáticos y la infiltración subrepticia en éstos como constante reto. No existe finalidad de dañar, espiar, defraudar o manipular.

Resulta difícil esbozar el perfil criminológico del mero intruso informático, debido a que se inserta en un ámbito de criminalidad con una gran zona oscura[3]. No obstante, del examen de los últimos hechos conocidos parece inferirse que se trata de personas altamente interesadas en el funcionamiento de los sistemas operativos.

[(3)]Por cifra oscura entendemos aquellos ámbitos de delincuencia en los que es difícil disponer de datos y estadísticas certeras.

Lectura recomendada

Podéis consultar: **Anónimo** (1998). *Máxima seguridad en Internet* (pág. 65 y ss.). Madrid.

La mayoría de ellos conocen a fondo tales sistemas, los lenguajes de programación y los protocolos de Internet (TCP/IP), aparte de los utilizados por otro tipo de redes. Dedican gran parte del tiempo a estudiar la existencia de agujeros (o puertas falsas) y fallos en dichos sistemas y a qué se deben. Una vez dentro de la máquina, el *hacker* ha logrado su propósito. No borran nada, excepto los *logs* que sean necesarios para hacer desaparecer su rastro. El *hacker* tiene como constante reto conseguir conocimiento y aprendizaje.

En un primer momento, se asoció la caracterización de estos intrusos a adolescentes de posición social media, inofensivos, con un coeficiente intelectual alto y aquejados por el síndrome de Robin Hood. Actualmente, y sin pasar por alto las dificultades inherentes al conocimiento de este ámbito, se considera que la mayor parte de comportamientos ilícitos relativos a la informática se llevan a cabo por personas vinculadas, de algún modo, a las empresas, esto es, empleados de confianza, programadores, técnicos, operadores, etc.

En cualquier caso, si bien parece haberse desechado la creencia de identificar al autor de estos delitos con genios capaces de acometer sofisticadas estrategias informáticas, lo que sí parece incuestionable es que **el denominador común estriba en el conocimiento de los sistemas informáticos y el incremento de la sofisticación del ataque**.

Lectura recomendada

Según un reciente estudio norteamericano, el 80% de los delitos informáticos tienen como autores a empleados de la propia empresa (denominados *insiders*), que, por lo general, buscan la venganza o el provecho ilícito. Para una relación detallada de *hackers*, actualmente vinculados relevantemente al mundo de la informática, podéis consultar (1998) *Máxima seguridad en Internet, op. cit.*, (pág. 76 y ss).

En cuanto a la dinámica de estas conductas, comparten las características de la criminalidad informática en general. Se trata de comportamientos poco arriesgados, susceptibles de ser ejecutados desde la oficina o el propio domicilio del intruso, que puede hallarse a pocos kilómetros, más allá de las fronteras del país donde se halla el ordenador al que accede, o, incluso, puede consistir en traspasar varias fronteras y varios ordenadores para dificultar su identificación y detección hasta acceder al objetivo final, que, paradójicamente, quizá radique en el propio lugar donde se halla el *hacker*.

Asimismo, es habitual que se logren borrar todas las huellas o rastros que permiten averiguar que la intrusión ha existido. De ahí la dificultad en el descubrimiento, persecución y futura represión de tales conductas. Un sector de la doctrina manifiesta que existe una especial intercomunicación entre este colectivo, mediante los denominados *electronic bulletin boards systems*, lo cual parece incrementar la peligrosidad de estos hechos.

En resumen, las conductas de *hacking* o mero intrusismo informático deben entenderse como comportamientos de **acceso no autorizado** a un sistema informático o red de comunicación electrónica de datos, desprovistos de cualquier intención distinta a la de conseguir dicha intromisión.

En algunas ocasiones, se hace referencia a estas conductas con la expresión *hacking blanco* para aludir a esa falta de intención delictiva ulterior al mero acceso.

Definidas y acotadas conceptualmente las conductas de *hacking*, corresponde examinar si se hallan reguladas en nuestro derecho. Al respecto, hay que decir que el acceso no consentido no ha estado previsto en el ordenamiento penal español hasta el momento. Sin embargo, se produjo una reforma del Código penal, que entró en vigor el 23 de diciembre del 2010, cuya finalidad es incorporar el castigo de estos comportamientos como delito. Vamos a explicar la situación antes y después de la reforma.

5.10.2. Encaje en el Código penal español, con carácter previo a la reforma de 2010

Como se acaba de señalar, las conductas de mero intrusismo informático, esto es, conductas de acceso no autorizado a sistemas informáticos, despojadas de cualquier elemento subjetivo ulterior y distinto al acceso mismo, no han gozado de una protección específica y autónoma en el nuevo Código penal.

Sin embargo, esa falta de tipificación expresa no ha supuesto la impunidad, en todo caso, de accesos no autorizados a un sistema informático ajeno. Se ha dicho ya que **si los accesos** no autorizados son concebidos como **medio comisivo para obtener resultados ulteriores más graves** (es decir, el acceso persigue un propósito ulterior y la intrusión se concibe como un medio necesario para atacar otros intereses), **encuentran encaje en los correspondientes delitos**.

Ahora bien, desprovistas de esa intención ulterior y más grave, lo cierto es que estas conductas de acceso inconsentido a un sistema sólo admitían un encaje muy forzado en algunos preceptos, cuya aplicación suscitaba serios problemas. Los partidarios de castigar estas conductas proponían dos ámbitos delictivos de aplicación:

1) Delitos contra la intimidad

Algunos autores entienden que estos delitos resultan aplicables, puesto que consideran el *password* como un dato personal que integra la intimidad.

Aun así, subsiste el problema de que estos delitos exigen que el autor obre con el ánimo de descubrir la intimidad, intención de la que, en principio, está desprovista la conducta del intruso.

Actividad

Discutid en el foro las siguientes cuestiones:

¿Creéis que la contraseña integra el derecho a la intimidad?

¿Se os ocurre alguna comparadción con la realidad analógica?

¿Es una llave lógica?

En este sentido se pronuncian las siguientes resoluciones judiciales:

a) Auto de 29.1.2002 (J.I. n.° 2 Lorca) (caso Ministerio del Interior)
b) Sentencia de 28.5.1999 (J.P. n.° 2 Barcelona) (caso Hispahack)

2) Delito de robo

Algunos autores entienden que, al tratarse de un apoderamiento de datos, puede llegar a entenderse como un delito de robo de información.

El delito de robo se halla previsto en los artículos 237 y ss. del Código penal:

> Artículo 237.
>
> Son reos del delito de robo los que, con ánimo de lucro, se apoderaren de las cosas muebles ajenas empleando fuerza en las cosas para acceder al lugar donde éstas se encuentran o violencia o intimidación en las personas.
>
> Artículo 238.
> Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:
> **1.°** Escalamiento.
> **2.°** Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.
> **3.°** Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.
> **4.°** Uso de llaves falsas.
> **5.°** Inutilización de sistemas específicos de alarma o guarda.
>
> Artículo 239.
> Se considerarán llaves falsas:
> **1.°** Las ganzúas u otros instrumentos análogos.
> **2.°** Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.
> **3.°** Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.
> A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

El delito de robo no protege la intimidad, sino el patrimonio de las personas físicas.

El principal problema que plantea considerar el intrusismo como un apoderamiento de información o llaves lógicas es que el Código define y acota el concepto de llave, en los arts. 238.4 y 239 CP:

> Y sólo los dispositivos mencionados expresamente en estos artículos pueden integrar el concepto de llave.

Por tanto, en resumen, estas conductas no tenían cabida en el Código penal español. Sin embargo, como se ha dicho ya, se ha producido una reforma del Código destinada a introducirlas. Esa reforma ha sido motivada, en gran medida, por normativa europea que resumimos a continuación.

5.10.3. La regulación de estas conductas en la Unión Europea

Las crecientes amenazas e incidentes sobre las propias infraestructuras informáticas, cuando son atacadas con el objetivo de alterar o impedir el normal funcionamiento de los sistemas de información, ha motivado la aparición de abundante normativa en la materia, a nivel europeo e internacional.

En el ámbito europeo, según se ha señalado anteriormente, se aprobó la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero del 2005, relativa a los ataques contra los sistemas de información. Esta Decisión Marco pretende aproximar el derecho penal de los Estados miembros mediante una definición europea común de los delitos contra los sistemas de información, con el fin de evitar los vacíos jurídicos y las diferencias de regulación, y garantizar así la cooperación policial y judicial respecto a estas infracciones.

Conforme a la Decisión Marco, los Estados miembros deberán sancionar como infracción penal:

1) el **acceso ilegal** a los sistemas de información,
2) la **intromisión ilegal en estos sistemas**,
3) y la **intromisión ilegal en los datos**.

En los tres supuestos se permite que las conductas de menor gravedad no estén sujetas a sanción penal.

En este momento, sólo nos ocuparemos de la primera de ellas. El acceso ilegal a los sistemas de información consiste en un acceso intencional y no autorizado al conjunto o a una parte de un sistema de información.

Artículo 2: **Acceso ilegal a los sistemas de información**:

1) Cada Estado miembro adoptará las medidas necesarias para que el **acceso intencionado sin autorización** al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

2) Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente **cuando la infracción se cometa transgrediendo medidas de seguridad**.

La Decisión Marco, sin embargo, faculta a los Estados para que consideren punible esta conducta únicamente cuando el **acceso se realice vulnerando medidas de seguridad**.

Así pues, la entrada en vigor de la Decisión Marco (16 de marzo del 2007) obligaba a reformar el Código penal español desde hace ya tiempo.

En la Decisión Marco, se prevén además dos circunstancias agravantes que, como sabéis, si concurren determinan que la pena sea más grave.

Agravantes (artículo 7):

1) Que el ilícito se cometa en el marco de una organización delictiva.

2) Cuando ocasione graves daños o afecte a intereses esenciales.

En ambos casos, la pena será de dos a cinco años de prisión.

5.10.4. El nuevo delito del art. 197.3 del Código penal

La reforma del CP del 2010 ha introducido en el título X, destinado a proteger el derecho a la intimidad, un nuevo apartado, el 197.3, que establece lo siguiente:

> "El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo 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."

A continuación, se destacarán algunos elementos que pueden generar problemas respecto de este nuevo delito, que, en principio, pretendía regular las conductas de *hacking*.

1) En primer lugar, este delito se ha ubicado en el título X, destinado a los delitos contra la intimidad, lo que condiciona la identificación del valor protegido, así como la interpretación de los distintos elementos del delito.

Respecto de la primera de las cuestiones apuntadas (identificación del valor que se protege), sin duda, **se ha considerado que el bien jurídico protegido con el castigo de estas conductas es el derecho a la intimidad** y, en concreto, a la intimidad informática, frente a un nuevo tipo de riesgos, a saber, los suscitados por las conductas de acceso no autorizado a un sistema.

Sin embargo, tal como se han definido estas conductas, no parece que el bien jurídico protegido deba ser necesariamente la intimidad, puesto que el autor no persigue su vulneración. Antes bien, si tuviéramos que identificar qué se

quiere proteger al introducir estas conductas en el Código, más bien parece que se trataría de un nuevo valor, como la seguridad del sistema o de los sistemas informáticos.

Por ejemplo, puede llevarse a cabo un acceso no autorizado a un sistema de una empresa, o de una administración pública, o de AENA, etc., sin que ninguna de estas potenciales víctimas tengan intimidad.

2) En segundo lugar, por lo que atañe al objeto sobre el que ha de recaer la conducta, el art. 197.3 castiga el acceso sin autorización **a datos o programas informáticos contenidos en un sistema informático** o en parte del mismo, mientras que la Decisión Marco se refiere al acceso **al conjunto o a una parte del sistema informático**, sin mención expresa de los datos.

Por tanto, se trata de dos cuestiones distintas y la interpretación del nuevo 197.3 CP puede generar problemas. En efecto, en la interpretación del contenido de este elemento caben, pues, dos posibilidades:

a) Un entendimiento de los datos restringido a los datos o información necesaria para el correcto funcionamiento de los sistemas, lo que resultaría una interpretación forzada y contraria a la ubicación del precepto.

b) Una interpretación del concepto de datos en toda su extensión, hipótesis que, sin embargo, desencadena algunas contradicciones. Así, por ejemplo, se produce un solapamiento con el vigente art. 197.2 CP, que castiga, con pena privativa de libertad de uno a cuatro años y multa de doce a veinticuatro meses, a quien, sin estar autorizado, acceda por cualquier medio a los datos registrados en ficheros o soportes informáticos, electrónicos o telemáticos.

Hubiera sido más adecuado que el Código aludiese a los accesos a sistemas informáticos sin mención expresa de los datos, asumiendo el concepto de sistemas propuesto por la Decisión Marco, que comprende los datos y programas indispensables para que los sistemas funcionen correctamente.

En definitiva, aunque el propósito de la reforma era introducir las conductas de acceso a sistemas, lo que se ha previsto es el acceso a datos o programas contenidos en sistemas, lo que puede generar problemas. En este sentido, habrá que esperar a la interpretación que hagan los tribunales de este nuevo precepto para saber si las conductas de mero acceso (desprovistas de otra intención más grave) tienen cabida en el nuevo art. 197.3 CP o, por el contrario, siguen siendo impunes.

Concluido el examen de los delitos vinculados a la criminalidad informática que prevé el Código penal, debéis tener presente que si un administrador de sistemas es víctima de cualquiera de estos delitos o descubre que el sistema que administra está siendo utilizado como plataforma de distribución de co-

pias de programas no autorizados o de pornografía infantil, **debe ponerlo en conocimiento de las fuerzas de seguridad y denunciarlo inmediatamente**, teniendo en cuenta el protocolo de actuación siguiente:

Anexo de los ficheros *log* relacionados con el delito cometido.

Si la acción se ha producido a través del correo electrónico, es necesario adjuntar las cabeceras completas del correo recibido.

Si se ha producido un delito de daños, es necesario adjuntar una valoración de los daños ocasionados.

Actuar con rapidez.

Resumen

En este módulo, se ha tratado de facilitar los conocimientos necesarios para que un profesional de la informática (un administrador de sistemas, por ejemplo) sepa cuáles son las obligaciones y, por tanto, las responsabilidades en las que puede incurrir a causa de su trabajo.

Se ha pretendido, asimismo, proporcionar los instrumentos teóricos indispensables para que estos profesionales logren identificar las conductas constitutivas de infracciones administrativas o penales, a fin de que, si dichas acciones tienen por objeto los sistemas que administran, puedan detectarlas y denunciarlas.

Actividades

1. ¿Creéis que los prestadores de servicios de Internet están obligados a mantener los registros log? ¿Debe adoptarse alguna medida de seguridad sobre dichos ficheros en caso de que los almacenen? ¿Creéis que es necesario que se regule su conservación? ¿Para qué?

2. Si vuestro jefe os pide que le mostréis el contenido del buzón de correo personal de un trabajador, ¿está cometiendo un delito o se trata de una conducta permitida? ¿Estáis obligados a hacerlo?

Ejercicios de autoevaluación

1. El servidor almacena datos de carácter personal. Si no se protegen con algunas medidas de seguridad, ¿se incurre en responsabilidad? ¿De qué tipo?

2. ¿Creéis que la tenencia y el uso de algún software de grabación (Nero)] que permite vulnerar la protección que algunos soportes (CD, DVD) incluyen para hacer copias privadas constituye un delito contra la propiedad intelectual (artículo 270.3 CP)? ¿Incurre en responsabilidad el fabricante, el usuario, los dos o ninguno?

Solucionario

Ejercicios de autoevaluación

1. Si no se adoptan las medidas de seguridad correspondientes en la protección de ficheros con datos de carácter personal, se infringe una de las obligaciones de la LOPDP y de su Reglamento de desarrollo (RD1720/2007). Así pues, se comete una infracción de tipo administrativo.

2. Una vez vendido el dispositivo (software, grabadoras), el fabricante no puede controlar el uso que de él hace el usuario. Por tanto, será una conducta punible si dichos dispositivos son susceptibles sólo de uso ilícito: medios específicamente destinados. El Nero permite usos lícitos, por tanto, no constituye delito contra la propiedad intelectual.

En realidad, se produce una confusión de estos delitos con las previsiones del nuevo art. 286 CP, que castiga el uso de dispositivos para liberalizar teléfonos móviles, descodificar canales de TV: delito contra los intereses económicos de los prestadores de servicios. Pero, en estos casos, generalmente se trata de instrumentos específicamente destinados (diseñados o adaptados para hacer posible dicho acceso).

Glosario

administrador de sistemas *m y f* Persona encargada de la informática, que a menudo desempeña todas las funciones, pero, en especial, la de administrador de servidores y la de administrador de usuarios, y, a veces, también la de jefe de informática.

CP *m* Acrónimo de Código penal.

delito *m* Conducta que atenta contra un bien jurídico, descrita como tal en el Código penal, a la que se asocia una sanción penal.

orden civil *m* Se resuelven conflictos entre particulares (filiación, matrimonio, contratos, etc.).

orden contencioso-administrativo *m* Se dirimen conflictos entre los particulares y las administraciones, o bien entre administraciones.

orden penal *m* Se enjuician delitos y faltas (infracciones previstas en el Código penal, que suponen las lesiones más graves de los bienes jurídicos).

orden social *m* Se resuelven cuestiones laborales (conflictos entre empresarios y trabajadores, despidos, contratos de trabajo).

Bibliografía

Gutiérrez, M.ª L. (1991). *Fraude informático y estafa*. Madrid. Ministerio de Justicia.

Littlejohn Shinder, D. (2003). *Prevención y detección de delitos informáticos*. Madrid: Anaya.

Morales, F. (2001). "La intervención penal en la Red. La represión penal del tráfico de pornografía infantil: Estudio particular". *Derecho penal, sociedad y nuevas tecnologías*. Madrid: Colex.

Morón Lerma, E. (2002). *Internet y derecho penal: Hacking y otras conductas ilícitas en la Red*. Pamplona: Aranzadi.

Orts, Enrique; Roig, M. (2001). *Delitos informáticos y delitos comunes cometidos a través de la informática*. Valencia: Tirant lo Blanch.

Rovira del Canto, E. (2002). *Delincuencia informática y fraudes informáticos*. Granada: Comares.