LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN. IMPLICACIONES LEGALES

José Pedro Morais Gallego
Centro de Formación e Recursos de Ourense

1. INTRODUCCIÓN

Cuando en 1978 la Constitución Española garantizaba el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, hacía una clara referencia a la limitación, mediante ley, del uso de la informática (artículo 18.4º). Posiblemente, en aquellos momentos, nadie era consciente de la repercusión que en el futuro iban a tener las nuevas tecnologías de la información y la comunicación.

La innovación tecnológica daría lugar a nuevos problemas sociales y políticos; la revolución informática cambiaría la estructura interna de la sociedad, alterando los métodos para conseguir y tratar la información, así como las técnicas de comunicación y trabajo.

Esta nueva sociedad, configurada en redes de información y más concretamente en *Internet*, se fundamenta en la virtualidad, que permite al usuario el derecho al anonimato y al proveedor de servicios el deber de disponer de medios para identificar los autores de actos ilícitos.

Es innegable el derecho fundamental del usuario de *Internet* a la intimidad y al secreto de las comunicaciones y este derecho se configura en el anonimato. No obstante, las conductas más dañosas realizadas a través de *Internet* y su entorno se fundamentan, precisamente, en la capacidad de que una persona digital, por medio de una identidad virtual generalmente anónima, vulnere el correo electrónico, los códigos de entrada a la información, la protección de programas informáticos, etc. e incluso pueda incurrir en la realización de los ilícitos penales más tradicionales (Morón, 2002).

Los poderes públicos intentaron a lo largo de estos años dar una respuesta a los cambios introducidos por las nuevas tecnologías en lo que se refiere al desarrollo de una legislación propia en materia informática.

En el inicio de los años 70, las primeras reacciones en materia legislativa iban en torno a la protección de la vida privada ante las nuevas posibilidades de recogida, almacenamiento, transferencia e interconexión de datos personales que propiciaba la informática.

A partir de los años 80, se pretende combatir la delincuencia económica específica derivada de las actividades relacionadas con las nuevas tecnologías, observando las dificultades

que presentan las disposiciones sobre la propiedad para la protección de una realidad inmaterial no tangible. De este modo, surgen las iniciativas legislativas en relación con la propiedad intelectual, para la protección de los programas de ordenador por medio del derecho de autor.

Más adelante, la actividad legislativa caminaba hacia la introducción de innovaciones en el campo del derecho procesal, perfeccionando la investigación de este nuevo tipo de delincuencia para, en la actualidad, centrarse en el derecho internacional por el hecho de que en la utilización de las nuevas tecnologías las fronteras desaparecen y la persecución de la llamada *criminalidad informática* tiene un carácter supranacional (Lourenço, 2003).

En este estudio se describen ciertas actividades, de dudosa o palpable ilicitud, relacionadas con la utilización de las nuevas tecnologías de la información y de la comunicación, haciendo un análisis de las respuestas del ordenamiento jurídico, bien ante las modernas modalidades delictivas o bien ante nuevos modos de la realización de las figuras más clásicas.

2. DIFERENTES PROCEDIMIENTOS DE ACTUACIÓN POR MEDIO DE LAS NUEVAS TECNOLOGÍAS

Los comportamientos de los usuarios de las nuevas tecnologías son variados, estando en continua evolución. En la denominación de estas conductas se aprecia una desmesurada proliferación de anglicismos, indicador claro del papel secundario que en estos momentos tiene la cultura hispánica en el sector de las tecnologías de la información y de la comunicación (Tabarés, 2003). Los procedimientos más habituales se describen a continuación.

2.1. Sniffing

Consiste en la utilización de programas rastreadores o *sniffers*, usados para supervisar el tráfico entre los ordenadores y buscar información. La utilización de estos rastreadores puede permitir el control invisible y no consentido del correo electrónico.

2.2. Snooping

Este tipo de acción es similar al *sniffing*. Además de interceptar el tráfico de la *red*, el autor accede a los documentos, correo y otro material guardado, realizando la copia de esa información a su propio ordenador.

El objetivo de esta conducta puede ser la simple curiosidad, pero también puede ser utilizado con fines de espionaje o robo de información o *software*.

2.3. Spoofing

El *spoofing* es una técnica para actuar en nombre de otros usuarios. Consiguiendo el nombre y la contraseña de un usuario legítimo e ingresando en

un sistema, se pueden efectuar acciones en nombre de ese usuario, tales como enviar falsos correos electrónicos.

La persona intrusa utiliza un sistema para obtener información e ingresar en otro, desde el que, a su vez, vuelve a entrar en otros sistemas. Este proceso es el llamado *looping*, que dificulta la identificación y la ubicación del atacante, ya que el recorrido sobrepasa de los límites de un país, y hace la investigación prácticamente imposible.

2.4. Rastreo o monitorización

La monitorización digital puede tener lugar a través de las denominadas *cookies*, o pequeños programas o subrutinas informáticas que identifican al usuario cada vez que entra en un servidor de información y que controlan en cierta medida sus preferencias, constituyendo una forma de intromisión en la privacidad informática de los usuarios.

Los denominados "programas espía" (*spyware, web bugs*), identificadores ocultos y otros dispositivos similares, son otras formas más graves de intromisión en la vida privada. Estos programas se introducen en el terminal de los usuarios sin su conocimiento accediendo a los datos, archivando información oculta o rastreando sus actividades.

2.5. Spaming

El *spaming* consiste en el envío no consentido de mensajes por correo electrónico a una multitud de particulares, publicitando productos o servicios comerciales. De este modo puede llegarse a la saturación de cualquier buzón de correo electrónico o incluso al mismo bloqueo de todo un sistema informático por medio de la ejecución de un programa de envío masivo de mensajes.

Como evolución de esta técnica, está la conducta de los *hoax*, que persiguen captar direcciones de correo y saturar la *red* o un servidor.

2.6. Cracking o "piratería informática"

Las conductas de *cracking* tienen como característica la eliminación o neutralización de los sistemas de protección que impiden la copia o utilización no consentida de una aplicación informática. Estaríamos, por lo tanto, ante una copia no autorizada y la posible distribución ilegal de programas informáticos (llamados *warez*, aplicaciones comerciales sometidas a la acción de un *crack*) con vulneración de los derechos de autor (Morón, 2002). Estas conductas serían diferentes a las conductas de mero intrusismo informático o *hacking*.

2.7. Conductas de "daños" o "vandalismo electrónico"

Consisten en asaltos sobre sistemas informáticos para ocasionar perturbaciones, modificar o destruir datos. Estos comportamientos reciben

diversa nomenclatura y se materializan por medio de virus (programas que modifican aplicaciones) o gusanos (programas que se autopropagan por medio del correo electrónico). Estas aplicaciones aprovechan sistemas mal configurados, la vulnerabilidad de programas o los fallos de seguridad para la destrucción de datos o perturbación de sistemas, llegando en algunos casos a permitir el acceso remoto y el manejo del sistema infectado.

Como modalidad de estos comportamientos podemos considerar los llamados *troyanos*. Se trata de programas informáticos que se instalan en el ordenador enmascarados en otros programas ejecutables, de imagen o sonido. Una vez instalados pueden permitir el acceso remoto al sistema por medio de las llamadas "puertas traseras" (Tabarés, 2003).

De modo similar, las bombas lógicas, *logic bombs*, consisten en la introducción en un programa de un conjunto de instrucciones no autorizadas para que, en una determinada fecha o circunstancia predeterminada, se ejecuten de forma automática ocasionando el borrado o destrucción de la información almacenada, distorsionando el funcionamiento del sistema o paralizando el mismo de forma intermitente.

2.8. Intrusismo informático o hacking

Las conductas de *hacking* o simple intrusismo informático consisten en comportamientos de acceso o interferencia, sin autorización, en un sistema de tratamiento de la información.

Se puede clasificar el *hacking* como directo o indirecto. El primero consiste en el acceso no autorizado a un sistema informático con la finalidad de obtener una satisfacción personal o intelectual por el desciframiento de los códigos de acceso o *passwords*, sin causar daños inmediatos, o bien por la voluntad de curiosear o divertirse. También es denominado como *joy riding*, o paseo de diversión, siendo propio de personas jóvenes, expertas en informática, sin motivación de causar daños (Libano, 2000).

En cuanto al *hacking* indirecto, se considera como un medio para la comisión de otros delitos como fraudes, sabotajes, piratería, etc. En este caso existe una intención de dañar, defraudar, etc. Estas conductas de intrusismo pueden dar lugar a ciertas especificidades:

- Introducción de datos falsos o *data diddling*, como por ejemplo la manipulación de transacciones de entrada en un sistema informático con la finalidad de ingresar movimientos falsos total o parcialmente, o eliminar transacciones verdaderas.
- Redondeo de cuentas, *salami*, o *rounding down*, introduciendo ciertas instrucciones en los programas para reducir sistemáticamente pequeñas cantidades

y transferirlas a cuentas distintas o proveedores ficticios abiertas con nombres supuestos y controladas por el defraudador (Blossiers, 2002).

- Recogida de información residual o *scavenging*, aprovechando la finalización de las ejecuciones de los programas realizados para la obtención de la información residual de la memoria o de los soportes magnéticos; también llamado *trashing*, o busca de directorios y contraseñas rastreando la *papelera* del sistema.

2.9. Phreaking

Esta conducta es realizada por personas con ciertas herramientas y conocimientos de *hardware* y *software* manipulando los sistemas informáticos de las compañías de telefonía con la finalidad de hacer llamadas sin costes.

El *phreaking* comenzó como una actividad íntimamente ligada al *hacking*, puesto que un *hacker* necesitaba hacer *phreaking* para poder utilizar mucho tiempo la línea telefónica de forma gratuita y, de la misma forma, un *phreaker* precisaba el acceso no consentido a un sistema de comunicaciones (Borghello, 2004).

2.10. Phishing

Consiste en el envío masivo de mensajes electrónicos que semejan ser notificaciones oficiales con la finalidad de obtener datos personales y bancarios de los usuarios para hacerse pasar por ellos en diversas operaciones *on line.* Mientras el internauta cree estar dando los datos a su banco de confianza, en realidad los está facilitando a una *web* duplicada similar o igual a la verdadera página de la entidad bancaria.

2.11. Linking, inlining, deep linking y framing

a) *Linking* es la utilización ilícita de hipervínculos. Se produce cuando una página *web* reproduce textualmente los títulos de los contenidos de otra página con enlaces al correspondiente contenido.

b) *Inlining* es un comportamiento similar al *linking*, referido a las imágenes (fotografías, dibujos o pinturas) que circulan libremente por la *red*. Consiste en copiar en una página *web* propia las imágenes de otras páginas que pagaron derechos de autor por ellas.

c) *Deep linking*. Este término hace referencia a la introducción en nuestra *web* de un *link* (enlace) la otra página *web* que no es la página de inicio o "*homepage*". Esta especie de "enlaces profundos" no poseen por el momento implicaciones legales claras, pero repercuten en los ingresos por publicidad, ya que los usuarios no pasan por la página de inicio (Blasco, 2004).

d) *Framing*. Consiste en el establecimiento de vínculos por medio de *frames*. La pantalla de la página *web* original se mantiene abierta, apareciendo una pantalla reducida con otra página, a la que se accede o reproduce sin permiso del autor o autores de la misma (Miró, 2005).

Como variedad de estas técnicas, los *pop ups*, son una forma de bombardear al usuario con publicidad no solicitada a través de ventanas emergentes cada vez que se visita una página *web*.

2.12. Caching y mirroring

El *caching* es una forma de copia de una página *web* que consiste en el almacenamiento intermedio y provisional de materiales en un sistema, guardando en la memoria RAM de un ordenador, mediante la realización de una copia, un archivo o conjunto de archivos para su posterior recuperación (Garrote, 2001).

El *mirroring* es la creación de sitios idénticos a otros existentes, pero no tan próximos al usuario. Lo básico de esta conducta reside en copiar de forma exacta una página *web* y colocarla en otro servidor más inmediato, a la que el usuario puede acceder con mayor facilidad. Este comportamiento afecta claramente a los intereses de los titulares de los derechos de la propiedad intelectual, puesto que limitan el acceso a la página original.

2.13. Softlifting

Se trata de la copia en diferentes ordenadores de un mismo usuario, empresa o institución, de un *software* del que se posee una sola licencia de uso. Dentro de este comportamiento también podría integrarse la adquisición de un programa de ordenador y su comunicación pública en una *red* interna para la utilización por parte de varios usuarios.

Esta conducta podría considerarse como una infracción contractual, por incumplimiento de las condiciones de una determinada licencia de *software*, además de una infracción de los derechos de explotación exclusiva de la propiedad intelectual (Mirón, 2005).

2.14. Downloading y uploading

Básicamente estas actividades consisten en la carga y descarga de archivos digitales que contienen obras protegidas polos derechos de autor.

Downloading sería la conducta del usuario que descarga en su ordenador una obra digitalizada, como puede ser un disco con canciones convertidas en archivos con formato *Mp3*. Como se trata de la simple reproducción de una obra, estaríamos ante una actividad lícita y permitida, siendo ilícita su puesta la disposición del público en general e incluso delictiva si concurre ánimo de lucro.

Uploading es la puesta la disposición de terceros de los archivos

digitales para la posterior descarga por parte de otros usuarios. Este comportamiento es claramente ilícito, puesto que se trata de una comunicación pública de obras protegidas por los derechos de autor.

2.15. Otras conductas

Parece ser interminable el abanico de comportamientos, de evidente ilegalidad o de dudosa legalidad, relacionado con el mundo de las nuevas tecnologías de la comunicación y de la información. Para finalizar, podemos considerar:

- Acceso a las áreas no autorizadas o *piggynbaking*, que consiste en el acceso a áreas restringidas dentro de los sistemas o dispositivos periféricos como consecuencia de puertas abiertas o dispositivos desconectados.
- Divulgación no autorizada de datos o *data leakcage*, consistente en la substracción de información confidencial almacenada en un sistema desde un punto remoto.
- Suplantación de personalidad o *impersonation*, bien mediante utilización de claves ajenas de acceso a un sistema, llaves o tarjetas magnéticas.
- Pinchado de líneas informáticas o *wiretapping*, se trata de interferir las líneas de transmisión de datos, recuperando la información que circula por ellas.
- *Carding*, o conductas de manipulación de tarjetas de crédito pertenecientes a otras personas con la finalidad de cometer fraudes.
- Robo de servicios o de tiempo, como utilización sin autorización alguna de los elementos informáticos de la empresa u organismo para la realización de trabajos para terceros o para beneficio particular.
- Técnicas de ingeniería social, basadas en la buena fe de las personas que facilitan contraseñas o claves solicitadas por alguien que se hace pasar por otro.
- Conductas de connotación sexual, especialmente las relacionadas con la pornografía infantil por *Internet*.

3. DELITOS INFORMÁTICOS Y DELINCUENCIA INFORMÁTICA

La complejidad de todas estas acciones se refleja, en un primer lugar, en la dificultad de conseguir una posición doctrinal unánime en cuanto a una denominación común a las mismas. En segundo lugar, y ya desde una perspectiva jurídica, existen también dificultades a la hora de encuadrar determinadas conductas en un tipo delictivo concreto.

Así, se utilizan los términos de delincuencia informática, criminalidad

informática, delincuencia de cuello blanco, abuso informático, *cybercrimen*, delito electrónico, *computer crimen* (en el ámbito anglosajón), *computerkriminalität* (expresión alemana).

En el año 1985, un grupo de expertos convocado por la OCDE para analizar este tipo de comportamientos, hizo referencia a ellos como "delitos relacionados con los ordenadores", integrados por cualquier conducta antijurídica, antiética, o no autorizada, relacionada con el procesamiento automatizado y/o transmisión de datos.

Obviamente, no todas las conductas anteriormente descritas, aunque muchas pueden ser socialmente reprochables, constituyen necesariamente un delito. Para que una acción sea calificada delictiva es preciso que esté tipificada como tal en la legislación penal correspondiente. En este sentido, el artículo 25.1º de la Constitución Española establece que "*nadie puede ser condenado o sancionado por acciones u omisiones que en el momento de producirse no constituyan delito, falta o infracción administrativa, según la legislación vigente en aquel momento*". De la misma forma, el vigente Código Penal de 1995 indica en su artículo 10 que "*son delitos o faltas las acciones y omisiones dolosas o imprudentes penadas por la ley*".

Son múltiples las definiciones de lo que puede constituir un delito informático. Así, Davara indica que consiste "en la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, sea *hardware* o *software*" (Davara, 1997).

Según Gómez Peral se trataría del "conjunto de comportamientos dignos de reproche penal que tienen por instrumento u objeto los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos" (Gómez, 1994).

Lo relevante es que, bajo las distintas denominaciones, se hace referencia a un tipo de actividades o comportamientos que tienen como instrumento u objeto algún elemento informático y que, lo más importante desde el punto de vista del derecho, reúnen los requisitos que delimitan el concepto de delito.

No obstante, algunos autores niegan la existencia del concepto "delito informático", prefiriendo denominar a las citadas conductas como "delincuencia informática" o "criminalidad informática", por el hecho de que tal fenomenología delictiva no ataca otros objetos de tutela ya protegidos, tratándose de nuevos modos de agresión y comisión de actividades ilícitas contra bienes jurídicos ya reconocidos y tutelados (Mata, 2001).

Otros autores, teniendo en cuenta los nuevos intereses surgidos de los desafíos de la sociedad actual, consideran que existen otros bienes jurídicos a proteger, tales como la información en sí misma y el interés colectivo en la seguridad y fiabilidad de los sistemas y redes de almacenamiento, tratamiento, procesamiento y transferencia de la misma. Por este motivo avalan la existencia del concepto de "delito informático" con entidad propia (Rovira, 2002).

De cualquier forma, estamos ante el nuevo reto de las nuevas tecnologías que, proporcionando evidentes beneficios, son susceptibles de riesgos e inseguridad y obliga a los poderes públicos a establecer formas de control de estos medios.

4. LOS PODERES PÚBLICOS ANTE LOS NUEVOS HECHOS DELICTIVOS

Considerando la información como bien jurídico a proteger o el posible ataque a los bienes jurídicos tradicionales a través de la informática, los poderes públicos recurren al Derecho Penal como medio de sanción de las nuevas conductas delictivas.

Este recurso al Derecho Penal como respuesta a la aparición de *Internet* y de las nuevas tecnologías, en opinión de R. Mata, presenta tres problemas fundamentales.

En primer lugar, hay que determinar la zona punible, decidir los hechos que tienen importancia penal entre los múltiples comportamientos irregulares derivados de las nuevas tecnologías.

Un segundo problema es la individualización de la responsabilidad criminal en el ámbito de los hechos cometidos a través de *Internet*. Es dificultosa la determinación individual de la responsabilidad dentro de la pluralidad de sujetos que aparecen en el contexto general de la *red*.

Además, existen ciertas limitaciones en la persecución de estos hechos motivadas por la fragmentación y aplicación territorial del Derecho, por la transnacionalidad de sus efectos, lo que lleva a una necesidad de armonización de la legislación y a una mayor cooperación internacional (Mata, 2004).

En el marco del Consejo de Europa, en Budapest, el 23 de noviembre de 2001, se firmó el Convenio sobre la Ciberdelincuencia con el objetivo de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a las nuevas manifestaciones de la delincuencia, adoptando una legislación adecuada y fomentando la cooperación entre los distintos Estados.

En el preámbulo de este Convenio se indica la necesidad de prevenir los actos dirigidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de esos sistemas, redes y datos,

mediante la tipificación de los mismos para la lucha efectiva contra esos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional.

El Convenio, pese a estar firmado por más de treinta países, no está en vigor por no contar con el número necesario de ratificaciones; no obstante, representa por el momento el instrumento internacional más válido para hacer frente a las conductas relativas a la llamada *cibercriminalidad* (Mata, 2004).

Este instrumento internacional clasifica en cuatro grandes grupos las conductas que constituyen ilícitos penales y que son un referente de cara a la adopción de medidas a nivel internacional:

A) Infracciones contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Dentro de estas conductas, figuran:

- acceso deliberado e ilegítimo a la totalidad o parte de un sistema informático,
- interceptación ilícita, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático,
- comisión deliberada e ilegítima de actos que causen daños, borren, deterioren o alteren datos informáticos,
- interferencias en los sistemas que obstaculicen gravemente el funcionamiento de los mismos mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos,
- conductas abusivas relativas a la producción, venta y obtención para su utilización de dispositivos informáticos que permitan la realización de los hechos delictivos anteriores.

B) Delitos relativos a la falsificación y el fraude informático. Los Estados deberán adoptar las medidas necesarias para tipificar como delito en su derecho interno las siguientes infracciones:

- introducción, alteración, borrado o supresión de datos informáticos que den lugar a datos no auténticos, con la intención de ser tenidos en cuenta o utilizados a efectos legales como si fueran auténticos,
- conductas de introducción, alteración, borrado o supresión de datos informáticos o cualquier interferencia en el funcionamiento de un sistema informático con la intención fraudulenta o delictiva de obtener de modo ilegítimo un beneficio económico.

C) Delitos relativos a los contenidos. En este grupo se hace referencia a una serie de conductas relacionadas con la pornografía infantil:

- producción, oferta o puesta la disposición de pornografía infantil por medio de un sistema informático,
- difusión o transmisión de pornografía infantil por medio de un sistema informático,
- adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona,
- posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

A estos efectos, en el Convenio, se entiende como pornografía infantil todo el material pornográfico que contenga la representación visual de un menor comportándose de una forma sexualmente explícita, la de una persona que parezca un menor comportándose de ese modo e incluso las imágenes realistas que representen menores en comportamientos sexualmente explícitos.

D) Delitos relacionados con infracciones de la propiedad intelectual y derechos afines. Los Estados deberán adoptar las medidas necesarias para tipificar como delito en su derecho interno las infracciones relativas a:

- la propiedad intelectual, de conformidad con las obligaciones del Acta de París de 1971 por la que se revisó el Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la propiedad intelectual,
- la protección de artistas intérpretes o ejecutantes, productores de fonogramas y organismos de radiodifusión (Convención de Roma).

5. LA RESPUESTA DEL ORDENAMENTO JURÍDICO ESPAÑOL

5.1. Ámbito penal

Según el Código Penal de 1995 y su modificación por la Ley Orgánica 15/2003, de 25 de noviembre, se pueden clasificar las conductas delictivas relacionadas con las nuevas tecnologías de la comunicación y de la información como:

a) Delitos contra la intimidad y la propia imagen

b) Delitos contra el patrimonio y el orden socioeconómico (hurtos, defraudaciones, daños, propiedad intelectual e industrial, mercado y consumidores)

c) Falsedades documentales

d) Otras referencias indirectas (defraudaciones de fluido eléctrico y similares, delitos societarios y daños).

Así, dentro de los delitos contra la intimidad, la integridad y dispo-

nibilidad de datos y sistemas informáticos, el artículo 197 del Código Penal (CP) castiga con penas de 1 a 7 años de prisión y multa de 12 a 24 meses el descubrimiento y revelación de secretos, como conducta que lleva a apoderarse de mensajes de correo electrónico ajenos o acceso a documentos privados sin la autorización de sus titulares. El artículo 264.2 CP castiga, como un delito de daños, con una pena de 1 a 3 años de prisión y multa de 12 a 24 meses, la destrucción, alteración o daño de programas o documentos electrónicos ajenos contenidos en *redes*, soportes o sistemas informáticos. El artículo 278 CP, en relación con el mercado y los consumidores, señala penas de 2 a 5 años de prisión y multa de 12 a 24 meses para el que se apodere o difunda documentos o datos electrónicos de empresas [1].

En relación con los delitos de estafa y fraude, el artículo 248.2 CP impone penas de 6 meses a 3 años de prisión para las estafas como consecuencia de manipulaciones informáticas, cuando lo defraudado excede de 400 €. El artículo 255 CP castiga con multa de 3 a 12 meses la defraudación de energía o en las telecomunicaciones valiéndose de mecanismos, alteración de contadores o medios clandestinos. Por otra parte, la utilización de cualquier equipo terminal de telecomunicación sin consentimiento de su titular, causando un perjuicio económico superior a los 400 €, está castigada con pena de multa de 3 a 12 meses (artículo 256 CP) [2]

Con respecto a los delitos relacionados con la propiedad intelectual e industrial, el artículo 270 CP señala la pena de 6 meses a 2 años de prisión y multa de 12 a 24 meses para la copia no autorizada de programas de ordenador o de música y para la fabricación, distribución o tenencia de programas que vulneran las medidas de protección anti-piratería. La misma pena establece el artículo 273 CP para el comercio a través de *Internet* con productos patentados sin la autorización del titular de la patente.

El acceso, sin consentimiento del prestador de servicios y con fines comerciales, a un servicio de radiodifusión sonora o televisiva y a servicios interactivos prestados a distancia por vía electrónica, así como la fabricación, importación, distribución, puesta a disposición, venta, alquiler o posesión de cualquier equipo o programa informático para hacer posible dicho acceso, está penado con 6 meses a 2 años de prisión y multa de 12 a 24 meses (artículo 286 CP). La misma pena impone este artículo para la alteración del número identificativo de los equipos de telecomunicaciones y el suministro, aun sin ánimo de lucro, de información sobre el modo de conseguir un acceso no autorizado a los citados servicios.

En relación con las conductas de exhibicionismo y provocación

sexual, el artículo 186 CP castiga con penas de 6 meses a 1 año de prisión y multa de 12 a 24 meses la venta, difusión o exhibición entre menores, por cualquier medio, de material pornográfico.

Con penas de 1 a 4 años de prisión sanciona el artículo 189 CP las conductas de producción, distribución, venta o exhibición por cualquier medio, de material pornográfico que utilice en su elaboración a menores de edad o incapaces, incluso está penada la simple posesión de material para la realización de estas conductas.

5.2. Ámbito civil y mercantil

La problemática que gira en torno a las nuevas tecnologías tiene sus repercusiones en el campo del derecho privado y, fundamentalmente, en el referente a la protección jurídica del *software*, derechos de autor, copia y distribución de programas, etc.

El artículo 428 del Código Civil (CC) indica que "el autor de una obra literaria, científica o artística, tiene el derecho de explotarla y disponer de ella a su voluntad", y remite a la legislación especial en el sentido de que "la ley sobre propiedad intelectual determina las personas a las que pertenece este derecho, la forma de su ejercicio y el tiempo de su duración. En los casos no previstos ni resueltos por dicha ley especial se aplicarán las reglas generales establecidas en este Código sobre la propiedad" (art. 429 CC).

Los programas de ordenador se consideran como la consecuencia de una actividad, con una notable carga de intelectualidad, que producen obras creativas, originales, que, bajo un determinado soporte, realizan ciertas tareas con la finalidad básica del manejo de la información (Davara, 2004). Así, como un bien inmaterial objeto del tráfico jurídico, nuestra legislación no ampara a los programas de ordenador bajo la protección de la propiedad industrial; la propia Ley de Patentes de 1986 indica en su artículo 4 que son patentables las invenciones nuevas y susceptibles de aplicación industrial, excluyendo de forma explícita a los programas de ordenador.

La normativa española a este respecto sigue el camino emprendido por casi todos los países del nuestro entorno, que es el de asimilar los programas de ordenador a las obras literarias, científicas o artísticas típicas de la propiedad intelectual. De forma inequívoca, el Real Decreto Legislativo 1/1996, de 12 de abril, Texto Refundido de la Ley de Propiedad Intelectual (LPI), señala como objeto de propiedad intelectual, entre diversas creaciones literarias, artísticas y culturales, a los programas de ordenador (art. 10).

Internet facilita la copia, distribución y puesta a disposición de obras musicales, videográficas, programas de ordenador, etc. Las conductas más conflictivas son las relaciona-

das con la copia y reproducción no autorizada de esas obras como, por ejemplo, la colocación de un programa de ordenador en un sitio *web* para hacer posible su copia a todos los que tengan acceso al mismo.

Como ya quedó apuntado en el tratamiento penal de estas conductas, la posibilidad del anonimato y la dificultad de la prueba de las mismas complican la aplicación del Derecho.

Los derechos de explotación de una obra o programa de ordenador durarán toda la vida del autor y setenta años después de su muerte o declaración de fallecimiento (arts. 26 y 98 LPI). No obstante, una obra ya divulgada podrá reproducirse sin la autorización del autor, para uso privado y siempre que la copia no sea objeto de utilización colectiva ni lucrativa (arts. 31 y 100 LPI).

A estos efectos, se consideran infractores de los derechos de autor a los que, sin autorización del titular de los mismos, pongan en circulación o tengan, con fines comerciales, una o más copias de un programa de ordenador conociendo o pudiendo presumir su naturaleza ilegítima. También son infractores de los derechos de autor los que pongan en circulación o tengan, con finalidad comercial, cualquier instrumento para facilitar exclusivamente la supresión o neutralización no autorizada de cualquier dispositivo técnico utilizado para proteger un programa de ordenador (art. 102 LPI).

El titular de los derechos de autor, sin perjuicio de otras acciones legales que le correspondan, podrá instar el cese de la actividad ilícita, la retirada del comercio de las copias ilegales y su destrucción, la inutilización o destrucción de los elementos exclusivamente destinados a la reproducción de esas copias y de cualquier instrumento destinado a facilitar la supresión o neutralización no autorizada de la protección de un programa de ordenador y también podrá exigir la indemnización de los daños materiales y morales causados (arts. 139 y 140 LPI).

5.3. Ámbito laboral

Desde el punto de vista de este estudio, la problemática de la aplicación de las nuevas tecnologías en el mundo del trabajo guarda una estrecha relación con lo que podría llamarse "uso indebido", es decir, aquel en que un trabajador no utiliza las tecnologías que el empresario o institución pone su disposición con una determinada finalidad, sino con un ánimo lúdico o basado en motivaciones personales. Se produce, en este caso, un vacío legal importante en el que existe la contraposición de los derechos de dos partes: por un lado, el poder de dirección del empresario sobre la actividad de los trabajadores a su servicio, y, por otro, el derecho a la intimidad y el secreto de las comunicaciones (Segoviano, 2003).

El empresario tiene reconocido el poder de dirección sobre la actividad de los trabajadores a su servicio, pudiendo adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por parte de aquellos de sus obligaciones y deberes laborales (art. 20.3º Estatuto de los Trabajadores –ET–).

El modo de llevar a cabo el control de las actividades de los trabajadores no está establecido de modo expreso. El citado artículo 20 ET indica que en la adopción y aplicación de las medidas de vigilancia el empresario debe guardar la debida consideración a la dignidad humana de los trabajadores. Por otra parte, en esta cuestión opera un límite de gran importancia referido a dos derechos fundamentales: el derecho a la intimidad (art. 18.1º CE) y el derecho al secreto de las comunicaciones (art. 18.3º CE), que pueden ser vulnerados por el empresario en su actividad de control de las obligaciones y deberes de los trabajadores.

Las resoluciones de los distintos Juzgados y Tribunales son dispares en relación con la utilización indebida por parte del trabajador de *Internet* y del correo electrónico y también a la hora de pronunciarse respecto a los poderes de control que tiene el empresario dentro de este ámbito (Segoviano, 2003). La línea jurisprudencial mayoritaria fue en un principio claramente favorable a los intereses de los empresarios, considerando que el derecho al secreto de las comunicaciones no ampara los correos electrónicos enviados polos trabajadores empleando los medios informáticos que la empresa pone su disposición, puesto que no se trata de una correspondencia personal, sino de la utilización indebida de medios e instrumentos de la empresa para fines ajenos a los estrictamente laborales. Igual sucede con el acceso a *Internet* en jornada laboral con una finalidad ajena a la derivada del puesto de trabajo, que priman los intereses del empresario ante el derecho a la intimidad del art. 18.1º CE.

Actualmente, en la jurisprudencia se aprecia un posicionamiento más favorable a los derechos de los trabajadores, prevaleciendo el derecho fundamental a la intimidad personal ante el interés empresarial por el hecho de obtener la prueba de un modo ilícito, tal como la utilización de programas espía sin conocimiento de los trabajadores o el registro del ordenador sin las garantías que establece el art. 18 ET de necesidad, respecto a la dignidad e intimidad y con asistencia de un representante legal de los trabajadores.

Ante este confuso panorama, muchas empresas implantan las llamadas *políticas de seguridad*, en las que se articulan las obligaciones y deberes de los trabajadores que disponen de acceso a los sistemas informáticos bien prohibiendo su uso, filtrando contenidos o vigilando las comunicaciones. En estas políticas se establecen las consecuencias que pueden tener para

los trabajadores el incumplimiento de esas medidas de seguridad en relación con el uso de *Internet* y del correo electrónico en el ámbito laboral.

6. A MODO DE CONCLUSIONES

Tras este recorrido por las distintas conductas relacionadas con la utilización de las nuevas tecnologías y de su encaje en el ordenamiento jurídico, se puede concluir que no todos los comportamientos que tienen como medio o finalidad elementos informáticos son necesariamente sancionables. Para que esto sea así deben concurrir ciertos requisitos establecidos previamente en las leyes.

Diariamente, estamos ante situaciones que, como consecuencia de un escaso desarrollo legislativo y de decisiones judiciales variadas, pueden generar cierta confusión. Se pretende, para finalizar, intentar dar respuesta a ciertos interrogantes que surgen en la vida cotidiana.

6.1. Copia privada de un CD

Estamos ante un supuesto legal en el que no es precisa la autorización del autor de una obra ya divulgada para proceder a una reproducción de la misma para el uso privado del copista, siempre que no sea objeto de utilización colectiva ni lucrativa. Por lo tanto, y tal como se desprende del artículo 31 LPI, hacer una copia de un CD o DVD para uso personal es un derecho y no constituye un delito.

6.2. Descargar de Internet software desprotegido o cracks

Descargar un fichero de música sin ánimo de lucro y para uso privado, no es delito; descargar un fichero de un libro sin ánimo de lucro y para uso privado, tampoco es delito; al igual que sucede con un fichero de una película, tampoco es delito siempre que no exista ánimo de lucro y sea para uso personal.

Descargar un programa informático, en el que su distribución no sea libre ni autorizada por su autor o distribuidor, sí sería delito porque, a diferencia de los otros tipos de ficheros, la descarga de *software* no está amparada por el derecho de copia privada (que permite la reproducción de obras ya divulgadas para uso personal del copista) y precisa la autorización del autor o distribuidor del *software*. Por lo tanto, la descarga de *software* tanto a través de una página *web* como por medio de las redes P2P es ilegal.

El artículo 100 LPI permite hacer una *copia de seguridad* de un programa de ordenador, pero sólamente por parte del que tiene el derecho a utilizar el programa, es decir, de su usuario legítimo. Por lo tanto, es importante la distinción entre copia privada, aplicada a una obra de audio o vídeo en formato informático, y copia de seguridad, aplicada exclusivamente a los programas de ordenador de los que el artículo 99 LPI prohíbe expre-

samente su copia incluso para uso privado, con la excepción vista de la copia de seguridad.

En cuanto a los denominados *cracks*, están prohibidos por toda la legislación e incluso su tenencia está penalizada.

6.3. Desprotección de CD y DVD para hacer una copia de uso privado

La desprotección de un CD o DVD para hacer una copia de uso privado no es un delito. El artículo 270.3º CP, en su nueva redacción según la Ley 15/2003, prevé el castigo de los que fabriquen, importen o simplemente tengan cualquier medio específicamente destinado a facilitar la supresión no autorizada o neutralización de la protección de los programas de ordenador o cualquier obra, pero hace una clara referencia a los términos previstos en el apartado 1º del mismo artículo "con ánimo de lucro y en perjuicio de tercero". Por lo tanto, la desprotección de un soporte con la finalidad de hacer una copia para uso privado y no colectivo no tiene carácter delictivo.

6.4. Difusión de obras musicales, literarias o científicas a través de páginas *web*

Los usuarios de sistemas similares al antiguo *Napster* realizan reproducciones lícitas cuando descargan a su ordenador obras protegidas para uso privado y no colectivo. No obstante, podemos considerar que, después, al poner a disposición de terceros dichas obras, están haciendo comunicaciones públicas ilícitas. Este comportamiento podría ser sancionable por la vía civil conforme a la LPI, pero no por vía penal a menos que la citada difusión se haga con ánimo de lucro.

Los titulares de la página *web*, por su parte, cometen uno ilícito civil cuando ponen a disposición del público obras de las que no son titulares, pudiendo convertirse esta conducta en delito en el caso de producirse una ganancia a cambio, bien directamente, bien indirectamente por medio de la publicidad o por el número de visitas (Miró, 2005).

6.5. Uso de las redes P2P (*Peer- to- peer*) en la descarga de archivos

El comportamiento de los usuarios de estas redes es similar al descrito en el punto anterior. En el antiguo sistema *Napster*, su página *web* servía como un intermediario que realizaba la puesta a disposición del público de las obras protegidas por el derecho de autor, existiendo una clara comunicación pública ilícita de las mismas, de la que los titulares de aquella *web* eran los responsables.

El sistema *Peer to peer* está basado en los mismos principios. No obstante, la página *web* en ningún momento pone a disposición del público las obras protegidas, sino que per-

mite a través del *software* que los usuarios contacten entre sí y, desde sus propios ordenadores, carguen y descarguen cualquier obra.

Las conductas de los particulares que acceden a estas redes tendrán la misma calificación legal que en el caso de *Napster*: la descarga es una reproducción de una obra, y dependerá de su uso (público o privado) para resultar ilícita. La puesta a disposición puede considerarse una comunicación pública ilícita, ya que permite al público el acceso a obras protegidas por el derecho a la propiedad intelectual (Miró, 2005).

La reforma del Código Penal, llevada a cabo por la Ley 15/2003, de 25 de noviembre, no dio una respuesta clara en torno al carácter delictivo de estas conductas. La exigencia de ánimo de lucro en las mismas implica delimitar el concepto de lucro; para ciertos sectores doctrinales el ánimo de lucro y el ánimo de ahorro son la misma cosa, el intercambio de archivos en una *red P2P* es un trueque, una forma de comercio. Además, se argumenta que una copia personal, al ser distribuida, deja de ser privada y no está amparada por el derecho de copia privada.

Desde otro punto de vista, una aplicación literal del Código Penal llevaría la siguiente paradoja: bajar una canción a través de una *red P2P* podría llevar a una pena de prisión de 6 meses a 2 años (art. 270 CP), pero el hurto de un CD entero en unos grandes almacenes, a una simple multa por la comisión de una falta (art. 623 CP).

La aplicación del Código Penal en estas conductas semiprivadas es difícil, salvo en casos de gran relevancia.

6.6. Compartir conexiones y accesos a sistemas de pago

Según el artículo 256 CP, la utilización de cualquier tipo de terminal de telecomunicación, sin el consentimiento de su titular y ocasionando a este un perjuicio superior a los 400 euros, está castigada con una pena de multa de tres a doce meses.

Por lo tanto, compartir conexiones y accesos a sistemas de pago puede considerarse delito siempre que tal práctica esté expresamente prohibida por el prestador de tales servicios u operadora y ocasione un perjuicio de más de 400 euros (*ver Nota 2*).

6.7. Aprovechar una conexión inalámbrica ajena

Esta conducta tiene un claro carácter delictivo. En primer lugar, se puede vulnerar el secreto de las comunicaciones y la intimidad del titular de esa conexión en los términos establecidos en el artículo 197 CP. Igualmente, se puede incurrir en un delito de defraudación (art. 255 CP) y, de la misma forma, se estaría cometiendo un delito de acceso no autorizado a un equipo de telecomunicación, con independencia de la cuantía de la posible defraudación (art. 286 CP).

6.8. Hacer público el modo de acceso no autorizado a un servicio de telecomunicaciones

El citado artículo 286 CP prohibe, aún sin ánimo de lucro, facilitar a terceros por medio de comunicación pública información sobre el modo de conseguir el acceso no autorizado a un servicio de radiodifusión sonora o televisiva y a los servicios interactivos prestados la distancia por vía electrónica.

6.9. Otras actividades relacionadas

Entre otras cuestiones relacionadas con las nuevas tecnologías, podemos considerar la descodificación de un canal de televisión mediante la utilización de un ordenador. Esta conducta constituye un delito, puesto que es precisa la utilización de un software específicamente orientado a romper una protección, con infracción del artículo 286 CP sobre el acceso no autorizado.

Para finalizar, es también delictiva la conducta de liberar un teléfono móvil, puesto que es preciso disponer de una tecnología (*software/hardware*) específicamente diseñada para la desprotección de los mismos. No obstante, el propio usuario puede liberar legalmente un teléfono móvil cuando lo hace con permiso o por delegación de la operadora correspondiente, tecleando los códigos suministrados por la misma.

7. BIBLIOGRAFÍA

Véase texto original en la versión gallega.

8. NOTAS

[1] El sistema de penas "días-multa" consiste en el abono de una cantidad fija de dinero diario durante un tiempo determinado. La extensión mínima de la multa será de 10 días y la máxima de dos años, en función del delito o falta y sus circunstancias. La cuota mínima diaria será de 2 euros y la máxima de 400 euros, en relación directa con la situación económica del reo.

[2] Cuándo la cantidad estafada o defraudada en relación con la energía, comunicaciones o equipos terminales de telecomunicación sea inferior a 400 euros, no constituye delito, pero sí falta, siendo castigada con la pena de localización permanente de cuatro a 12 días o multa de uno a dos meses.