# LA CIBERDELINCUENCIA EN EL DERECHO ESPAÑOL

MOISÉS BARRIO ANDRÉS (*)

SUMARIO: 1. INTRODUCCIÓN.—2. ¿EXISTEN LOS «DELITOS INFORMÁTICOS» O «DELITOS CIBERNÉTICOS»?.—3. PANORAMA COMPARADO E INTERNACIONAL.—4. LA CIBERDELINCUENCIA EN EL CÓDIGO PENAL ESPAÑOL.—5. LOS DISTINTOS DELITOS EN PARTICULAR.—6. CONCLUSIÓN.

(*) Letrado del Consejo de Estado. Profesor de Derecho Público, ICADE (Madrid). Abogado.

ABSTRACT

El presente trabajo aborda la problemática de los llamados «delitos informáticos». Se analiza, en primer lugar, su configuración dogmática. Seguidamente, se examina brevemente el derecho comparado e internacional en la materia, para pasar a estudiar con detalle el régimen jurídico en España y, particularmente, las modificaciones operadas tras la reforma del Código Penal mediante la Ley Orgánica 5/2010, de 22 de junio. Finalmente, en sede de conclusiones, se apuntan varias consideraciones críticas y se sugieren diversas líneas de reforma.

This paper addresses the problem of «computer crime». It analyzes, first, its dogmatic configuration. Next, examines the comparative and international law in this area, moving to study in detail the legal regime in Spain and particularly the modifications after the reform of the Criminal Code by Law 5/2010 of June 22. Finally, based on findings, it suggests several critical considerations and points out various lines of reform.

PALABRAS CLAVE

Delitos informáticos, delitos cibernéticos, hacking, cracking, ciberdelincuencia, delitos en internet.

Computer crime, cybercrime, hacking, cracking, cyber crime, internet crimes.

## 1. Introducción

Desde la publicación del libro de Hegel *La filosofía del Derecho* (1821), la distinción que el autor formuló entre «sociedad civil», es decir, el conjunto de las relaciones sociales concernientes a los intereses de los individuos, de los grupos y de las clases sociales, y la «sociedad política», el Estado, que atañe a los intereses de los ciudadanos y que gobierna a la sociedad civil mediante la Administración Pública compuesta por funcionarios públicos, se ha hecho cada vez mas conocida y ha sido aplicada con utilizaciones metodológicas distintas.

La galopante expansión de Internet ha multiplicado los problemas que suscita su utilización. Por ello, se puede decir que existe un desfase entre las dos formas de organización social indicadas, y que la evolución del Estado y del Derecho es más lenta que la de la organización de la sociedad civil. Esta realidad no pasa desapercibida al mundo jurídico, que asiste al resquebrajamiento de los esquemas tradicionales, imponiéndose una irresistible necesidad de adaptación a la nueva realidad. El Derecho debe amoldarse a la realidad (y no a la inversa), lo cual conlleva como una de sus funciones la de canalizar, por cauces adecuados, la nueva realidad social, económica y cultural en que se traducen los avances de Internet (1).

En 1963 se publicó el trabajo de Carbonnier titulado «*L'hypotese de non droit*» (2) , que posteriormente dio lugar a un Congreso de juristas que analizó los fenómenos del no-derecho: *hackers*, ocupadores de fábricas y otros fenómenos que generaban una auto regulación propia, pero al margen del Derecho. La doctrina cuestionó entonces si, en definitiva, Internet es un supuesto de no-derecho, dado que

---

(1) Así, base citar el impacto de las conexiones de banda ancha (DSL, cable, FTTH), redes inalámbricas (Wi-Fi, WiMax), dispositivos móviles, (ordenadores portátiles, PDA, telefonía móvil, smart phones), telefonía IP, discos de almacenamiento portátiles, servidores privados y virtuales, o en fin, la facilidad de que cualquier contenido (gráfico, texto, imagen o vídeo) pueda ser digitalizado y distribuido en masa (coadyuvado por programas y sitios webs dedicados al intercambio de archivos), por citar sólo alguna de las innovaciones tecnológicas cuyo uso resulta hoy generalizado.

(2) Jean Carbonnier, «*L'hypothése du non-droit*», en Archives de philosophie du droit, t. VIII, 1963, p. 55.

surgió como un foro de intercambio múltiple y libre de información, creado desde abajo (no por disposición de los Poderes Públicos) y que opera bajo el principio de libertad. Si bien inicialmente la Red se ha caracterizado por una ausencia de intervención legal y estatal, lo cierto es que hoy ya han sido superadas estas posiciones.

En efecto, el planteamiento no debe ser «Internet versus Derecho», de igual manera que no pueden contraponerse, como conceptos antagónicos, Derecho y Libertad. Sostener que Internet debe ser un espacio de «no-Derecho» para salvaguardar la libertad con la que surgió equivaldría a afirmar que en un Estado de Derecho no existe Libertad. Como recuerda VILLAR PALASÍ, Internet es ante todo «un espacio social y como tal debe ser regulado por el Derecho» (3).

Por ello, en las últimas décadas los Estados nacionales y la Comunidad Internacional han abordado la regulación de Internet. Lógicamente, el Derecho Penal no ha permanecido al margen de esta tarea, pues todo lo que es ilegal en el mundo real también lo es en el virtual. El pasar por Internet no legaliza ni exime a ninguna conducta de su encaje en el Ordenamiento jurídico. Sin embargo, Internet presenta una problemática propia motivada por la ausencia de un núcleo central de Gobierno y la dificultad de exigir responsabilidades a los autores de cualquier infracción.

A los efectos del Derecho Penal, existen determinadas técnicas y modos de proceder informáticos constitutivos de ilícito penal (a.e. acceso inconsentido a un sistema informático, interceptación ilícita de comunicaciones, interferencias en el sistema, prácticas de *phising*, ataques de denegación de servicio —DoS, DDoS—, abuso de dispositivos, fraude informático) y también ciertos contenidos cuya vulneración se ve facilitada por el medio Internet (v. gr. delitos de pornografía infantil, contra la propiedad intelectual e industrial o revelación de datos personales), para los cuales un sector doctrinal ha acuñado, no sin controversia, la categoría de «delitos informáticos» y que analizaremos seguidamente.

---

(3) José Luis VILLAR PALASÍ, «Implicaciones jurídicas de Internet», en *Anales de la Real Academia de Jurisprudencia y Legislación,* núm. 28, 1998, pp. 507 y ss.

## 2. ¿Existen los «delitos informáticos» o «delitos cibernéticos»?

A finales de los ochenta, algunos autores [Camacho Losa (4), García Moreno (5) o García Portero (6)] empezaron a hablar de un pretendido «delito informático», denominación importada del término anglosajón *computer crime*, aún cuando la legislación española no contemplaba ningún ilícito en materia tecnológica. Tal expresión fue felizmente abandonada por la doctrina tras las críticas vertidas por Correa en Italia o Tiedemann en Alemania.

Como sintetiza Romeo Casabona, «en la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de delitos en los que nos encontramos, como única nota común, su vinculación de alguna manera con los ordenadores, pero ni el bien jurídico agredido es siempre de la misma naturaleza ni la forma de comisión del hecho —delictivo o merecedor de serlo— presenta siempre características semejantes» (7) . En consecuencia, propone el autor el empleo de expresiones tales como «agresiones realizadas contra medios o sistemas informáticos, o a través de los mismos».

Por su parte, Gutiérrez Francés añade que «el sustantivo delito tiene significación específica para el penalista, que difiere de la que se otorga en el lenguaje coloquial, siendo precisa, al menos, su tipificación en la ley penal vigente» (8). De este modo, han ido surgiendo expresiones alternativas como criminalidad informática o delincuencia informática, según se quiera acentuar la vertiente criminológica o penal del fenómeno.

---

(4) Luis Camacho Losa, *El delito informático*, Góndor, Madrid, 1987.

(5) Luis García Moreno, «El delito informático», en *Revista Chip,* año III.

(6) Roberto García Portero, «Los delitos informáticos», en *Revista Latinoamericana de Derecho Penal y Criminología,* núm. 6, pp. 176 y ss.

(7) Carlos Romero Casabona, *Poder Informático y Seguridad Jurídica*, Fundesco, Madrid, 1987, p. 41.

(8) María Luz Gutiérrez Francés, *Fraude Informático y Estafa*, Ministerio de Justicia, Madrid, 1991, p. 12.

En cambio, los defensores de esta figura argumentan, como propugna DAVARA RODRÍGUEZ, que el «delito informático» es aquel en el que «la realización de una acción, que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software» (9). Sin embargo, lo que viene a poner de manifiesto esta corriente minoritaria es la comisión de acciones a través de elementos informáticos o vulnerando los mismos, sin aportar elementos privativos que sustantiven una nueva categoría penal.

En definitiva, no existe una categoría autónoma de «delitos informáticos» o «delitos cibernéticos». Además, el Código Penal español de 1995 no ha introducido el «delito informático», ni admite que exista como tal dicha figura. El *locus comissi delicti* puede ser un domicilio particular, una vía pública o la Red. Argumentar lo contrario significa crear una nueva clase de ilícitos no autorizada por el legislador, ni exigida tampoco por la naturaleza de las cosas. De ahí que se deba hablarse más bien de delincuencia informática que de «delitos informáticos» propiamente tales.

Ahora bien, los delincuentes han encontrado en Internet un campo especialmente abonado para la comisión de delitos, lo que exige una respuesta penal específica a estas conductas.

Así, la Red posibilita la distribución indiscriminada de contenidos ilegales o pornográficos, el espionaje y el acceso a información confidencial y personal de modo casi indetectable, la causación de daños y perjuicios de difícil cuantificación con una mínima infraestructura, o la proliferación de «ciberterroristas» y «ciberespías», por citar sólo unos ejemplos. Además, el mundo virtual ofrece mayores facilidades para la comisión de delitos: así las pruebas son endebles y fácilmente alterables, la lentitud en la tramitación de los procedimientos de investigación y enjuiciamiento favorece la destrucción o inutilización de las pruebas o, en fin, el enmascaramiento del au-

(9) Miguel Ángel DAVARA RODRÍGUEZ, *Derecho Informático*, Aranzadi, Madrid, 1993, p. 302.

tor y el empleo de «personalidades virtuales» arroja incertidumbre e impunidad en la identificación del delincuente (10). Igualmente, debemos apuntar que muchos de estos delitos no son descubiertos, son descubiertos tarde o por puro azar. En este sentido, existe una «macro-victimización» muy difícil de determinar y cuantificar.

El Derecho Penal debe, por tanto, responder ante estas nuevas amenazas haciendo uso de sus técnicas e instrumentos, pero sin olvidar sus principios estructurales y en especial el principio de *última ratio*. Hoy en día se enfatiza la necesidad de un sistema penal eficaz frente a las nuevas formas de criminalidad propias de un mundo globalizado. Pero el Derecho Penal no puede convertirse en un sistema que deseche la Justicia. El garantismo penal (11) cobra aquí máxima importancia.

Pero antes de analizar la regulación española realizaremos una breve referencia al marco comparado e internacional de la ciberdelincuencia.

## 3. Panorama comparado e internacional

Desde el campo penal, a nivel comparado se observan tres técnicas normativas: *a)* el recurso a Leyes penales especiales, *b)* la tipificación de nuevas figuras delictivas en el Código Penal y *c)* la elaboración de normas internacionales.

i) Han optado por la primera vía países como Francia, Gran Bretaña, Holanda, Estados Unidos, Chile o Venezuela, que han elaborado Leyes penales especiales para abordar este fenómeno. En Europa, Francia cuenta con una Ley relativa al fraude informático de 1988 (12) y Reino Unido promulgó en 1991 la Computer Misuse Act a raíz de un grave caso de *hacking*. En América, Estados Unidos

---

(10) En este punto véase la tesis doctoral de Eloy Velasco Núñez, *Delitos cometidos a través de Internet. Cuestiones procesales*, La Ley, Madrid, 2010. También Pablo García Mexía, *Derecho europeo de Internet*, Netbiblo, La Coruña, 2009.

(11) *Vid*. Luigi Ferrajoli, *Derecho y razón. Teoría del garantismo penal*, Trotta, Madrid, 2001.

(12) Ley núm. 88-19, de 5 de enero de 1988.

adoptó en 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030), que modificó al Acta de Fraude y Abuso Computacional de 1986. En Iberoamérica, sobresale la Ley chilena contra los delitos informáticos de 1993 (13), pionera de los países de ese entorno.

ii) En segundo lugar, la tipificación de nuevos delitos en el Código Penal ha sido la otra técnica empleada para hacer frente a este desafío. En Europa, Alemania, Austria, Italia, España y Portugal, y en América, Argentina y México son los principales exponentes.

iii) En tercer y último lugar, la dimensión transnacional también ha obligado a adoptar soluciones a nivel internacional. En el ámbito de las Naciones Unidas, debemos citar el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos, de 1977. En el ámbito del Consejo de Europa, destaca el Convenio sobre el Cibercrimen, aprobado en Budapest en 2001 y vigente desde julio de 2004. Y, por último, a nivel comunitario, el objetivo de armonización del Derecho Penal en la Unión Europea ha tomado un giro más decidido a partir de la firma del Tratado de Lisboa en 2007, que opta por la Directiva en vez de por la Decisión Marco para conseguir una mayor armonización de disposiciones relativas a las infracciones con dimensión transfronteriza de especial gravedad, entre las que se encuentra la delincuencia informática.

De todos estos instrumentos descolla principalmente el Convenio sobre la Ciberdelincuencia, adoptado en Budapest el 23 de noviembre de 2001 (14).

Dicho Convenio surge como consecuencia del desarrollo y utilización cada vez mayor de las tecnologías de la información y la comunicación y de las posibilidades consiguientes que ofrecen tales medios para la comisión de nuevos tipos de delitos, así como de la necesidad de aplicar una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, a cuyo fin ordena a las Partes la adopción de una legislación que dé respuesta adecuada a

---

(13) Ley núm. 19.223, sobre delitos informáticos.

(14) Sobre el mismo, puede verse Óscar Morales García, «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre Cyber-crime», en VVAA, *Delincuencia Informática. Problemas de responsabilidad*, Consejo General del Poder Judicial, Madrid, 2002, pp. 13 a 33.

tales nuevas formas de delincuencia informática y el establecimiento de una política de cooperación internacional. Se trata de un instrumento internacional pionero en el ámbito de los delitos cometidos por medio de Internet u otras redes informáticas, y pone un acento especial en la lucha contra la pornografía infantil, el fraude informático y las violaciones de seguridad en la Red.

El Convenio es el fruto de cuatro años de trabajo de los expertos de los 45 países miembros del Consejo de Europa y de no miembros como Estados Unidos, Canadá y Japón, y ha sido ratificado por España el 20 de mayo de 2010 (15), habiendo entrado en vigor en nuestro país el 1 de octubre de 2010.

El Convenio ha llenado un vacío en el Ordenamiento jurídico internacional y su entrada en vigor permite hacer frente a una criminalidad de nuevo orden, que utiliza las redes informáticas y condiciona y puede poner en peligro su desarrollo futuro. A diferencia de otros ámbitos en que el Derecho internacional armoniza legislaciones y prácticas nacionales preexistentes, en el ámbito de la cibercriminalidad ha sido paradójicamente el Derecho internacional el que impulsa la adopción de medidas nacionales.

Expuesto este marco, nos corresponde ocuparnos seguidamente de la legislación penal española sobre la materia.

## 4. La ciberdelincuencia en el código penal español

España, como acabamos de indicar, ha optado por regular la ciberdelincuencia en el propio Código Penal, desechando la opción de una Ley penal especial.

De esta forma, ni el Código Penal de 1995 o sus sucesivas reformas han destinado un Título o rúbrica específica, descartando el establecimiento de un capítulo específico dedicado a los «delitos informáticos» o de una norma común que facilite su adecuado tra-

(15) Instrumento de ratificación publicado en el *BOE* de 17 de septiembre de 2010.

tamiento y sanción. Además, existe una importante dispersión normativa, pues las distintas figuras están diseminados a lo largo del articulado del Código (arts. 186, 197, 211, 238.5, 248.2 y 3, 256, 270, 286, etc.), ubicándose en distintos capítulos en función de los bienes jurídicos en los que se ha decidido incluirlos. No se considera, pues, que exista ningún vínculo común entre ellos.

Recientemente hemos asistido a la promulgación de la vigesimocuarta reforma del Código de 1995, concretamente la operada por Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

La justificación de la reforma, según el propio Preámbulo de la norma, se concreta brevemente en dos postulados: *a)* primero, la necesidad de cumplir con previas obligaciones internacionales contraídas por España —ejemplos de ello son la introducción de la responsabilidad penal directa de las personas jurídicas, el reforzamiento de la lucha contra la corrupción o el tratamiento de la criminalidad organizada, entre otros— y; *b)* segundo, lo que denomina «el surgimiento de nuevas cuestiones que han de ser abordadas», fruto de «la cambiante realidad social».

La reforma continúa la tendencia expansiva y funcionalizadora del Derecho Penal, desconociendo que esta rama debe proteger únicamente los bienes jurídicos más importantes de los ataques más intolerables. El derecho punitivo es el último recurso para la represión y sanción de las conductas más perniciosas para el orden y la paz social. En virtud del principio de subsidiariedad, el Derecho Penal sólo deberá operar en aquellos casos en los que las demás parcelas del Ordenamiento no pueden ofrecer una tutela mínimamente satisfactoria. Como certeramente ha escrito Quintero Olivares, «esa huida sistemática al derecho punitivo como *refugium peccatorum* sólo puede explicarse como modo demagógico de satisfacer a la llamada opinión pública, mientras se desprecia o ignora que el grado de ineficacia consustancial al sistema penal resultará más patente y lamentable conforme se haga crecer el marco de las tareas que se le asignan» (16).

---

(16) *Vid*. Gonzalo Quintero Olvares, *La Justicia penal en España*, Aranzadi, Pamplona, 1996.

Por ello, las propuestas de expansión, a la par que de reducción del ámbito de garantías cuando se trata de un delincuente que pueda ser reputado como *enemigo* de la Sociedad, que paradójicamente se formulan en nombre de un novedoso Derecho Penal de la postmodernidad (17) no resuelven los problemas, sino que, por el contrario, generan una legislación cada vez más precipitada (18) y chapucera, caracterizada además por el descenso de su nivel de calidad técnica.

Y particularmente sobre la presente reforma, MESTRE DELGADO contundentemente ha valorado la misma, enseñando que: primero, se confirma el abandono de los procesos de despenalización que se plantearon en la década de los ochenta del siglo pasado, siendo evidente una «voluntad de huida al Derecho Penal»; segundo, se produce un «notable incremento punitivo» así como la incorporación de diez nuevas figuras delictivas, y; tercero, el Legislador sigue actuando en respuesta inmediata a fenómenos delictivos o sociales de trascendencia mediática, poniendo «el acento en el simbolismo de la norma penal por encima de su eficacia» (19).

Por lo que se refiere a la ciberdelincuencia, la reforma se ha limitado a introducir nuevos tipos y a reformar algunos ya existentes. Los principales tipos afectados por la reforma han sido el «hacking» o intrusión informática (art. 197 del Código Penal, en adelante CPEN), la estafa informática (art. 248 CPEN) y el «cracking» o daños informáticos, previsto en el artículo 264 CPEN. Todos ellos serán objeto de un análisis más detenido en el próximo epígrafe.

---

(17) Destaca la construcción del denominado *Derecho Penal del Enemigo*, desarrollado por JAKOBS, con invocación de textos de HOBBES (especialmente capítulo XXVIII de su *Leviathan*) y KANT (tanto en su *Die Metaphysik der Sitten* como en *Zum Ewigen Frieden*). En detalle, Günther JAKOBS y Manuel CANCIÓ MELIÁ, *Derecho Penal del enemigo*, Civitas, Madrid, 2003.

(18) La «motorización legislativa» —una expresión acuñada por Carl SCHMITT, «Die Lage der europaischen Rechtswissenschaft», en *Verfassungsrechtliche Aufsatze*, Duncker & Humbolt, Berlín, 1958— que parecía patrimonio del Derecho Administrativo, ya se ha extendido irremediablemente al Derecho Penal.

(19) Esteban MESTRE DELGADO, «Los cambios de paradigma punitivo en un nuevo proyecto de reforma penal», en *La ley penal, Revista de Derecho penal, procesal y penitenciario,* núm. 61, 2009, pp. 3 y ss. Más detalladamente, José Luis MANZANARES SAMANIEGO, *Código Penal. Adaptado a la Ley Orgánica 5/2010, de 22 de junio. Comentarios y Jurisprudencia*, 2 tomos, Comares, Granada, 2010.

La justificación de estas modificaciones, según se explica en su Preámbulo, ha sido «cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información», y se ha decidido incardinar las conductas punibles en apartados diferentes, al tratarse de bienes jurídicos diversos. El primero, relativo a los daños, donde quedan incluidos los consistentes en deteriorar o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno. El segundo apartado se refiere al descubrimiento y revelación de secretos, donde se incluye el acceso sin autorización, vulnerando las medidas de seguridad, a datos o programas informáticos contenidos en un sistema o en parte del mismo. Finalmente, por lo que se refiere al delito de estafa, se incorpora la cada vez más extendida modalidad consistente en defraudar utilizando las tarjetas ajenas o los datos obrantes en ellas, realizando con ello operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Tras estas consideraciones pasamos a examinar los diversos delitos, para cuya exposición los hemos sistematizado atendiendo a la estructura del Convenio sobre la ciberdelincuencia. Así, dividiremos las infracciones en cuatro grupos: I.- Delitos contra la confidencialidad, integridad y disponibilidad de datos o sistemas informáticos, II.- Delitos asociados a la informática, III.- Delitos de contenido, y por último, IV.-Delitos relativos a las infracciones contra la propiedad intelectual y derechos conexos.

## 5. Los distintos delitos en particular

### 5.1. *Delitos contra la confidencialidad, integridad y disponibilidad de datos o sistemas informáticos*

#### *a)* Intrusismo e interceptación de las comunicaciones (*Hacking*)

El artículo 197.1 del Código Penal castiga al que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de documentos o intercepte comunicaciones.

Las conductas cometidas en la Red integrantes de este tipo reciben el nombre de intrusismo informático o «hacking». Siguiendo a MORÓN LERMA, podemos definirlo como «el conjunto de comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o red de comunicaciones y a la utilización de los mismos sin autorización o más allá de la misma» (20).

Así, las prácticas más habituales incluyen el descifrado de contraseñas (*password guessing*), las creación de puertas traseras (*backdoors*), la instalación de caballos de Troya, trampas y bombas lógicas, la interceptación de los paquetes de datos (21) (*sniffers*), el acceso o control remoto o, en fin, la propagación de virus y gusanos, entre otros.

Con el objeto de poner fin a diversas lagunas, la reforma introduce un nuevo apartado 3 en el precepto, pasando los actuales apartados 3, 4, 5 y 6 a ser los apartados 4, 5, 6 y 7, y se añade un apartado 8, de modo que los cambios son los siguientes:

> «3. 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.
>
> Cuando de acuerdo con lo establecido en el artículo 31.bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66.bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras *b)* a *g)* del apartado 7 del artículo 33.
>
> [...]
>
> 8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado».

---

(20) Esther MORÓN LERMA, *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*, Aranzadi, Pamplona, 1999, p. 42.

(21) Los datos en una red basada en IP, como es Internet, son enviados en bloques conocidos como paquetes o datagramas.

La reforma da respuesta al llamado «hacking», consistente, como acabamos de señalar, en el acceso inconsentido al propio sistema informático o a informaciones ubicadas en el sistema o en la red de comunicaciones (bases de datos, software, etc.), sin permiso del titular y sin necesidad de móvil o acción posterior alguna. Se diferencia del «cracking» en que no causa daños o no inutiliza el sistema.

Se castiga, por tanto, el mero hecho de saltarse las barreras de seguridad informáticas (*firewalls*, sistemas de detección de intrusión IDS, etc.), que se reputa como un atentado contra el derecho a la «intimidad informática», pero siempre que exista como resultado un acceso o mantenimiento en el mismo sin autorización.

El acceso a los datos o software puede lograrse por cualquier medio o procedimiento, pero siempre vulnerando las medidas de seguridad establecidas para impedirlo, lo que permite concluir que la inexistencia de medidas de seguridad informática determina la atipicidad del acceso. El segundo tipo de este párrafo consiste en mantenerse dentro del sistema contra dicha voluntad.

En ambos casos se repite el requisito de la falta de una autorización cuyo titular no se indica, pero que debe entenderse en relación con quien pueda otorgarla, ya sea la persona a la que tales datos se refieren, ya sea el que tenga el legítimo derecho a la exclusión de terceros (22).

*b)* Protección de datos (*habeas data*)

El artículo 197.2 sanciona, al que sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar. La presencia de elementos normativos en el tipo hace necesario acudir a la legislación sobre protección de datos (la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, LOPD).

---

(22) Manzanares Samaniego, *op. cit.*, II, p. 316.

Este apartado, que no ha sido modificado, confiere protección penal a la *privacy* o intimidad, de conformidad con lo ordenado en el artículo 18 de la Constitución. Las nuevas tecnologías han menoscabado la configuración tradicional del derecho a la intimidad edificada por la doctrina civilista como derecho de reserva absoluto. El funcionamiento de la informática es incompatible con una prohibición absoluta del tratamiento de los datos, ante los múltiples e impredecibles flujos de información y procesos de *feedback* o retroalimentación que tienen lugar hoy en día.

En este contexto, la privacidad no puede seguir siendo definida como aquella esfera individual en la que se constata un «grado cero» de sociabilidad, pues de la misma dimanan no sólo facultades de exclusión de terceros sino también facultades de control sobre los datos personales informatizados existentes en los sistemas informáticos y en las redes telemáticas (STC 254/1993, de 20 de julio). El derecho a la privacidad deja de configurarse como un derecho negativo, de rechazo de las intromisiones, para pasar a contemplarse como un derecho positivo, de afirmación de la propia libertad y de limitación sobre el poder informático. La privacidad cuenta ahora necesariamente con una proyección social, de ahí que las facultades dimanantes de la misma sean designadas como «libertades informáticas» (STC 354/1993, FJ 7.º), que otorgan el derecho de control del uso de los datos personales incorporados en un fichero informático.

Surge así el *habeas data* como derecho de control sobre los datos (acceso, rectificación y cancelación de los mismos), interviniendo el Estado en su protección y tutela con Agencias o Comisarios para la Protección de los Datos. La expresión «habeas data» o «habeas scriptum» alude al derecho a la propia intimidad informática o, como señala la doctrina alemana, al derecho a la autodeterminación informativa (cfr. Sentencia del Tribunal Constitucional Federal alemán de 14 de diciembre de 1983).

El artículo 197.2 CPEN complementaría así la regulación administrativa contenida en la LOPD, estableciendo sanción a los ataques contra los «datos reservados de carácter personal o familiar». Sin embargo, la doctrina, casi de modo unánime, ha criticado el presente tipo, puesto que existe una tutela civil y administrativa suficiente

y, además, origina múltiples problemas a la hora de esclarecer las conductas penales (23). Lo más correcto hubiera sido reservar la represión penal para aquellos datos que *directamente* afectan a la privacidad del sujeto (datos sobre ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual), en tanto que la tutela administrativa de la LOPD operaría para el *resto* de datos personales. Sin embargo, esta interpretación no tiene cobijo en el Código, por cuanto que el artículo 197.6 CPEN alberga un tipo agravado para los supuestos de abuso informático sobre datos personales pertenecientes al núcleo de la privacidad —los que la LOPD denomina en su art. 7 «datos especialmente protegidos»— (datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual). De este modo, dado que el Código Penal prevé un tipo agravado para esta categoría de datos, *a sensu contrario* debe entenderse que los datos tutelados en el tipo básico son todos los demás, es decir, los no especialmente protegidos. En consecuencia, resulta forzoso que el Legislador opere un adecuado deslinde entre la tutela penal y administrativa siguiendo el principio de mínima intervención penal.

### *c)* Daños y sabotajes (*cracking*)

Integran esta categoría aquellos supuestos etiquetados como «vandalismo digital», el «ciberterrorismo» y también las de «cracking» dirigidos a la producción de daños.

Los delitos de daños constituyen las infracciones básicas entre las que tienen un contenido patrimonial pero no se orientan hacia el enriquecimiento del sujeto activo. No ofrece el Código de 1995 una definición de daño, a diferencia de lo que ocurría en el Código Penal de 1928, cuyo artículo 750 incluía en tal concepto la destrucción, el deterioro y la causación de cualquier perjuicio a otro en su patrimonio. Hoy, señala MANZARANES SAMANIEGO (24), suele considerarse el daño de modo similar, entendiendo por destrucción la pérdida total

---

(23) En detalle, Fermín MORALES PRATS, en Gonzalo QUINTERO OLIVARES y Fermín MORALES PRATS (dirs.), *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi, 8.ª ed., Pamplona, 2009, pp. 416 y ss.

(24) MANZARANES SAMANIEGO, *op. cit.*, II, p. 615.

del objeto, por inutilización la pérdida de su eficacia y por deterioro la pérdida parcial de la cosa o de su valor.

Respecto de los incidentes que se ejecutan sobre los «datos» o «programas informáticos», la conducta de «destrucción» implica la supresión o borrado total de los datos, la «alteración» se integra por comportamientos de inserción de datos, modificación o supresión parcial y la «inutilización» puede llevarse a cabo mediante la ocultación o la encriptación (25). La destrucción o modificación de datos o programas, puede ejecutarse mediante la introducción en el sistema de algún tipo de virus y, además, pueden asumir especial gravedad si la información confidencial se almacena en un programa de ordenador (así, por ejemplo, piénsese en el ataque al software de facturación o contabilidad de una empresa) (26).

En cuanto a los ataques que se lanzan contra los «sistemas de información», suelen concretarse en comportamientos dirigidos a ocasionar perturbaciones sobre los mismos, por ejemplo, mediante ataques masivos de denegación de servicio (DDoS). Estos ataques persiguen sobrecargar o saturar algunos de los recursos físicos del sistema objeto del ataque hasta hacerlo inoperativo (p. ej. memoria, espacio en disco duro, ancho de banda), logrando con ello el bloqueo o interrupción temporal de dicho sistema.

El legislador ha reformado el artículo 264, que queda redactado como sigue:

> «1. El que 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.
>
> 2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando,

---

(25) *Vid*. Mirentxu Corcoy Bidasolo, «Protección penal del sabotaje informático. Especial consideración de los delitos de daños», en *La Ley, Revista jurídica española de doctrina, jurisprudencia y bibliografía,* núm. 1, pp. 1000-1016.

(26) Morón Lerma, *op. cit*., pp. 43 y ss.

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.

3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

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

2.º Haya ocasionado daños de especial gravedad o afectado a los intereses generales.

4. Cuando de acuerdo con lo establecido en el artículo 31.bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrán las siguientes penas:

*a)* Multa del doble al cuádruple del perjuicio causado, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años.

*b)* Multa del doble al triple del perjuicio causado, en el resto de los casos.

Atendidas las reglas establecidas en el artículo 66.bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras *b)* a *g)* del apartado 7 del artículo 33».

El precepto ha experimentado un cambio radical con la reforma de 2010. Su anterior apartado 2 castigaba al que «por cualquier medio destruya, altere, inutilice o de cualquier modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos», y tenía por objeto cumplir con lo dispuesto en la Directiva 91/250/CE, del Consejo, de 14 mayo 1991, sobre la protección jurídica de programas de ordenador (hoy derogada por la vigente Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de los programas de ordenador), si bien ahora se le dota de un ámbito más amplio para cumplir con la Decisión marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques de los que son objeto los sistemas de información.

La Ley Orgánica 5/2010, de 22 de junio, opera dos importantes innovaciones: *a)* perfecciona la redacción anterior, perfilando mejor la conducta típica y; *b)* agrava la pena cuando el autor sea una or-

ganización criminal, la conducta sea de especial gravedad o quepa atribuir responsabilidad penal a una persona jurídica. Persigue el legislador evitar las lagunas que existían a la hora de subsumir algunas conductas de «cracking». El delito es de resultado, por cuanto requiere la producción de un resultado grave. Sin embargo, tal gravedad se compagina muy mal con la seguridad jurídica. El legislador debería haber concretado la gravedad, por ejemplo estableciendo la cuantía de los daños graves. Sin tal requisito la conducta sería impune.

*d)* Abuso de sistemas informáticos

El artículo 256 del Código Penal castiga al que hiciere uso de cualquier equipo terminal de telecomunicación (esto es, teléfono, fax, correo electrónico, etc.), sin consentimiento de su titular, ocasionando a este un perjuicio superior a 400 euros.

A nivel comparado, este delito venía a reprimir la utilización indebida de grandes superordenadores en una época en la que se facturaba por tiempo el uso de los mismos, aunque en España el debate parlamentario se centró en los abusos telefónicos del personal doméstico. En la actualidad, las conductas delictivas más frecuentes se refieren a defraudaciones telefónicas (p. ej. derivación de una línea de teléfono de otro titular, realización de llamadas sin autorización), el pirateo de contraseñas de acceso a servicios de pago (por ejemplo, bases de datos jurídicas o contenidos restringidos), causando un perjuicio patrimonial evidente a su legítimo titular.

Pero algunas de estas conductas plantean problemas de encaje en el tipo, dado que este exige un «uso de terminal de comunicaciones sin consentimiento del titular», lo cual no siempre se lleva a cabo en los supuestos reseñados (por ejemplo, el autor, tras obtener la contraseña de la víctima, accede al servicio desde su propio ordenador o desde otros equipos). Por ello, resulta criticable la idoneidad y oportunidad del tipo, puesto que existen adecuadas vías civiles de reparación, de modo que no debe acudirse al derecho punitivo para tutelar el equipo terminal de comunicaciones, lo cual también violenta el principio de intervención mínima del Derecho Penal.

### 5.2. *Delitos asociados a la informática*

Integran esta rúbrica las estafas y fraudes cometidos en Internet tipificados en el artículo 248 del Código Penal.

Desde que ANTÓN ONECA publicara en 1958 (27) su célebre trabajo definidor del delito de estafa, la imaginación del timador ha desarrollado un infinito abanico de posibilidades. Internet se revela como otro cauce añadido para obtener ganancias de modo sencillo. Algunos de sus supuestos más populares son los siguientes:

— Subastas en Internet: una vez enviado el dinero por el producto que se pujó y fue adjudicado, nunca se llega a recibir el mismo o se recibe otro en su lugar que no corresponde con el inicialmente ofertado y, por supuesto, de bastante menor valor.

— Ofertas de Proveedores de Internet con unas excelentes prestaciones a un precio muy atractivo, pero se establece un contrato de larga duración y complicado de romper ante la existencia de cláusulas contractuales penales.

— Uso no autorizado de tarjetas de crédito: en un apartado de la página web se solicita el número de la tarjeta bancaria del internauta con la excusa de comprobar si es mayor de edad (generalmente en sitios de contenido pornográfico), realizándose cargos no consentidos *a posteriori*.

— Marketing «multinivel», «en pirámide» o «en cadena»: consistente en promesas de comisiones monetarias por la venta de productos y servicios previamente adquiridos, o por porcentaje que reciba de los colaboradores que el propio internauta pueda captar, sin que en la práctica se obtengan los pretendidos ingresos, amén de constituir una práctica prohibida por la legislación mercantil.

— Ofertas del tipo «gane dinero trabajando desde casa» o «sea su propio jefe»: promesas muy atractivas para gestionar un «negocio redondo», con ganancias cómodas e inmediatas a cambio de una «mínima» inversión previa, y también oportunidades de inversión con anuncios del tipo «hágase rico en X días».

---

(27) José ANTÓN ONECA, Voz «Estafa», en *Nueva Enciclopedia Jurídica*, Francisco Seix, Barcelona, 1958, pp. 56 y ss.

— Prestación de servicios inexistente, especialmente servicios turísticos «fantasma»: compañías fraudulentas falsean paquetes de viajes, ofreciendo transporte, alojamiento y servicios de inferior calidad a la pagada, o que cobran por conceptos nunca contratados.

— Servicios de Atención Sanitaria y productos «milagro», ofreciendo remedios infalibles o tratamientos curativos de escasa o nula eficacia terapéutica (la mayoría de ellos se basan en el «efecto placebo») a precios que duplican o triplican su verdadero coste. También se incluyen aquí la venta de medicamentos falsificados, muy destacadamente anabolizantes.

La estafa informática constituyó una de las novedades más destacables del Código Penal de 1995. Fue una respuesta al uso criminal de las nuevas tecnologías y puso fin a la polémica doctrinal acerca de si una máquina puede ser engañada. Como se dice en la STS 860/2008, de 17 de diciembre, «la redacción del art. 248.2 del Código Penal permite incluir en la tipicidad de la estafa aquellos casos que mediante una manipulación informática o artificio semejante se efectúa una transferencia no consentida de activos en perjuicio de un tercero admitiendo diversas modalidades, bien mediante la creación de ordenes de pago o de transferencias, bien a través de manipulaciones de entrada o salida de datos, en virtud de los que la máquina actúa en su función mecánica propia».

La reforma ha modificado el artículo 248, que queda redactado como sigue:

> «1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
>
> 2. También se consideran reos de estafa:
>
> *a)* Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
>
> *b)* Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.
>
> *c)* Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen

operaciones de cualquier clase en perjuicio de su titular o de un tercero».

La novedad consiste en una ampliación puntual de la estafa informática, añadiéndose la utilización de tarjetas de crédito, débito o cheques de viaje para realizar operaciones de cualquier clase en perjuicio del titular de dichos medios de pago o de terceros. Se cierra así la laguna existente en estas defraudaciones que utilizan los citados instrumentos de pago o los datos obrantes en ellos, realizando con esa información, incluso sin necesidad de utilizar materialmente la tarjeta, operaciones de cualquier clase en perjuicio de su titular. La reforma en este punto resulta muy acertada y da cumplimiento a la Decisión marco del Consejo, de 28 de mayo de 2001, relativa a la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo.

### 5.3. *Delitos de contenido*

Pertenecen esta categoría aquellos delitos que persiguen la creación, publicación y distribución de contenidos ilegales.

De Miguel Asensio (28) distingue entre *a)* «contenidos nocivos o perjudiciales para el receptor» y *b)* «contenidos ilícitos». Los primeros son aquellos que, sin ser delictivos, pueden resultar ofensivos o inadecuados para el destinatario por incluir opiniones, creencias o juicios de valor que pueden agraviar al destinatario. En cambio, pertenecen a la categoría de «contenidos ilícitos» cualesquiera que contravengan la ley.

El Derecho Penal sólo deberá interesarse por aquellos contenidos tipificados como delito. El resto de contenidos ilícitos deberán ser tutelados por las restantes ramas del Ordenamiento (v. gr. en los excesos a la libertad de información que son difundidos a través de una página web, la protección al perjudicado se articula conforme a

(28) Pedro Alberto de Miguel Asensio, *Derecho Privado de Internet*, Civitas, Madrid, 2001, pp. 538 y ss.

la Ley Orgánica 1/1982, de 5 de mayo). Por lo que se refiere a las conductas punibles, se engloban aquí la distribución de pornografía infantil o la apología de la violencia, terrorismo, racismo o xenofobia. Además, también conforman esta categoría las injurias y calumnias vertidas en la Red.

Sin embargo, la reforma se ha centrado en relación a los delitos sexuales, introduciendo varias modificaciones.

En primer lugar, ha incorporado un nuevo artículo 183.bis, con la siguiente redacción:

> «El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño».

Este precepto es fruto de una enmienda del Grupo Popular en el Congreso que experimentó, no obstante, algún cambio (29). Su tipificación también resultada obligada por cuanto que el Convenio sobre el Cibercrimen establece la necesidad de adoptar medidas contra delitos cometidos contra o a través de Redes informáticas, entre otros, la pornografía infantil.

Las nuevas tecnologías han supuesto una mayor dificultad de los padres para la vigilancia de las personas adultas con quienes sus hijos se relacionan. Internet permite que los menores de edad se comuniquen, sin salir de su habitación, con cualquier desconocido de cualquier parte del mundo. Cada vez es más frecuente que los pederastas sustituyan las visitas a los parques infantiles por los chats de Internet para buscar a sus víctimas. Aparecen así nuevas formas de-

---

(29) *Vid*. MANZARANES SAMANIEGO, *op. cit*., II, p. 255.

lictivas como el «grooming informático», esto es, el acoso a menores vía *online*, que constituye un delito preparatorio de otro de carácter sexual más grave y consiste en acciones emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, al crearse una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él(30).

La reforma de 2010 acertadamente aborda el fenómeno de la proliferación de comunicaciones por Internet con menores de edad por parte de personas sin escrúpulos con la finalidad de concertar encuentros para la comisión de delitos de carácter sexual prevaliéndose del engaño. El nuevo tipo consta de varios elementos. Al contacto con el menor de trece años a través de alguno de los medios señalados debe seguir no sólo la propuesta para concertar un encuentro orientado a la comisión de los delitos especificados, sino también la realización de actos materiales de acercamiento.

En segundo lugar, suprime el apartado 8 del artículo 189 y modifica el primer párrafo y las letras *a)* y *b)* del apartado 1 y el primer párrafo del apartado 3, que quedan redactados como sigue:

> «1. Será castigado con la pena de prisión de uno a cinco años:
> *a)* El que captare o utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.
> *b)* El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por

(30) Vicente Magro Servet, «El "*grooming*" o ciber acoso infantil, el nuevo artículo 183.bis del Código Penal», *Diario La Ley,* núm. 7492, Sección Tribuna, 20 de octubre de 2010.

También Joseph María Tamarit Sumalla, «La protección penal del menor frente al abuso y la explotación sexual», en *Análisis de las reformas penales en materia de abusos sexuales, prostitución y pornografía de menores*, Colección de Monografías Aranzadi, Aranzadi, 2.ª ed., Navarra, 2002, y Fermín Morales Prats, «Los ilícitos en la red (II): pornografía infantil y ciberterrorismo», en Carlos Romeo Casabona (dir.), *El cibercrimen nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Comares, Granada, 2006.

cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

[...]

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

[...]

8. (Suprimido)»

El cambio obedece a la necesidad de tipificar nuevas conductas de acuerdo con la Decisión Marco antes citada. Es el caso de la captación de niños para que participen en espectáculos pornográficos o la conducta de quien se lucra con la participación de aquéllos.

Finalmente, la admisión de la responsabilidad penal de las personas jurídicas en la Ley Orgánica 5/2010, de 22 de junio, determina la inserción de un artículo 189.bis, subtipo especial para los delitos comprendidos en el capítulo V (prostitución y corrupción de menores), cuando el responsable sea una persona jurídica, asignándose importantes penas de multa y la posibilidad de imponerles las penas recogidas en las letras *b)* a *g)* del apartado 7 del artículo 33 (disolución, suspensión de actividades, clausura de locales, prohibición de realizar actividades en cuyo ejercicio se hubiera cometido, favorecido o encubierto el delito, inhabilitación para obtener contratos y ventajas fiscales o de la Seguridad Social e intervención judicial).

### 5.4. *Delitos relativos a las infracciones contra la propiedad intelectual y derechos conexos*

Esta última categoría engloba a los delitos de comisión más habitual en Internet, por lo que realizaremos aquí un breve apunte de los mismos. Son los delitos contra la propiedad intelectual tipificados en los artículos 270 y siguientes de nuestro texto punitivo: reproducir, plagiar, distribuir o comunicar públicamente, una obra literaria, artística o científica, o su transformación, sin la autorización de los titulares de los correspondientes derechos.

Con carácter general, debe notarse que la peculiar naturaleza de los derechos relativos a la propiedad intelectual permite que sobre un mismo objeto (libro, partitura, escultura, programa de ordenador, etc.) puedan concurrir intereses que, a veces, pueden llegar a ser contrapuestos. El autor de la obra dispone de una amplia gama de facultades de su derecho de propiedad que puede transmitir o ceder según múltiples modalidades, lo cual, a su vez, originará nuevos titulares de derechos que, como tales, pueden tenerse también como perjudicados por el delito (31).

Además, en el campo de la propiedad intelectual hay que destacar dos fenómenos importantes: la internacionalización de su protección y la existencia de Organizaciones sectoriales dedicadas a velar por estos derechos (la más importante es la Organización Mundial de la Propiedad Intelectual, OMPI; en España, la Sociedad General de Autores y Editores, SGAE), lo cual en ocasiones genera problemas de legitimación para actuar en el proceso penal, puesto que no sustituyen plenamente al autor en el ejercicio de las acciones penales.

También hay que recordar que la informática se manifestó desde sus prolegómenos como un medio eficaz para la vulneración de estos contenidos. Inicialmente las violaciones se referían exclusivamente a los programas de ordenador, pero la irrupción de nuevos soportes —tales como el CD-ROM o el DVD— ha permitido extender el objeto material del delito a todo tipo de obras, surgiendo la figura del llamado «top manta» (actividad consistente en la venta no autorizada de obras en la calle). Finalmente, la cuestión tiene su punto álgido y polémico con las descargas de contenidos a través de Internet, para lo cual la Disposición final cuadragésima tercera de la Ley 2/2011, de 4 de marzo, de Economía Sostenible ha introducido un procedimiento especial para la interrupción de la prestación de servicios de la sociedad de la información y para la retirada de contenidos que vulneren la propiedad intelectual (32).

La protección penal de las obras frente a diferentes acciones (reproducción, plagio, distribución, comunicación, transformación,

---

(31) En detalle, Concepción Carmona Salgado, *La nueva Ley de Propiedad Intelectual*, Montecorvo, Madrid, 1988.

(32) Lo analizamos en Moisés Barrio Andrés, «Luces y sombras del procedimiento para el cierre de páginas web», *Diario La Ley,* Sección Tribuna, 2 de febrero de 2011.

interpretación, ejecución, importación, exportación, almacenamiento, etc.) requiere acudir a los preceptos de la Ley de Propiedad Intelectual, cuyo Texto Refundido fue aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y ha sido modificado en diversas ocasiones posteriores.

La Ley Orgánica 5/2010, de 22 de junio también se ha ocupado de los delitos contra la propiedad intelectual e industrial, que naturalmente pueden cometerse utilizando cualquier soporte y, por tanto, el electrónico. En este caso, el legislador ha reaccionado contra la excesiva punición operada en la reforma de 2003. El Preámbulo de la reforma lo explica así:

> «El agravamiento penológico operado por la Ley Orgánica 15/2003, de 25 de noviembre, en el ámbito de los delitos relativos a la propiedad intelectual e industrial ha evidenciado una cierta quiebra de la necesaria proporcionalidad de la pena en el caso de conductas consistentes en la venta a pequeña escala de copias fraudulentas de obras amparadas por tales derechos, máxime cuando frecuentemente los autores de este tipo de conductas son personas en situaciones de pobreza, a veces utilizados por organizaciones criminales, que con tales actos aspiran a alcanzar ingresos mínimos de subsistencia. Por ello, añadiendo un párrafo segundo al apartado 1 del artículo 270 y modificando el apartado 2 del artículo 274, para aquellos casos de distribución al por menor de escasa trascendencia, atendidas las características del culpable y la reducida cuantía del beneficio económico obtenido por éste, siempre que no concurra ninguna de las circunstancias de agravación que el propio Código Penal prevé, se opta por señalar penas de multa o trabajos en beneficio de la comunidad. Además, en tales supuestos, cuando el beneficio no alcance los 400 euros la conducta se castigará como falta».

En consecuencia, opera dos cambios. En primer lugar, añade un párrafo segundo al apartado 1 del artículo 270, que tendrá 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 treinta

> y uno a sesenta días. En los mismos supuestos, cuando el beneficio no exceda de 400 euros, se castigará el hecho como falta del artículo 623.5».

La atenuación penal introducida se presenta como una excepción al párrafo primero, de forma que en los casos de distribución al por menor y siempre que se cumplan los restantes requisitos, el Juez podrá imponer la pena de multa de tres a seis meses o, alternativamente, trabajos en beneficio de la comunidad de treinta y uno a sesenta días. Se trata, por tanto, de una adecuada rectificación de la huida al Derecho Penal con el establecimiento de dos penas menos graves para dicha conducta, en la línea de los últimos pronunciamientos judiciales en el sentido de considerar el denominado *top manta* como «el último eslabón del comercio ilegal, a través de personas que solo buscan un medio de ganarse la vida».

En efecto, se han ido dictando una serie de sentencias (sobre todo, a partir de la Sentencia de la Audiencia Provincial de Barcelona 180/2006, de 8 de febrero) sobre propiedad intelectual con relación a los vendedores callejeros de CD de música y DVD con copias irregularmente obtenidas, en las que se atempera la reacción penal contra ese tipo de conductas. Esas sentencias se apoyan en la del Tribunal Supremo, de 24 de febrero de 2003, que señala que «para determinar en qué casos habrá de acudirse al derecho penal y qué conductas serán merecedoras de una mera sanción administrativa, ha de partirse del principio de intervención mínima que debe informar el Derecho penal en un moderno Estado de derecho. Sólo ante los ataques más intolerables será legítimo el recurso al derecho penal». Aplicando tal doctrina, varias de las sentencias que han absuelto a los denominados «manteros» han afirmado que no toda infracción del derecho de exclusividad del titular de la propiedad intelectual tiene cabida en el artículo 270 del Código Penal. «Sólo las conductas más graves, como la reproducción en masa de su obra artística amparada por el derecho, o su distribución en grandes cantidades pueden configurar el delito. La venta callejera es el último eslabón del comercio ilegal, y no tiene entidad suficiente para justificar la aplicación del derecho penal» (la ya citada Sentencia de la Audiencia Provincial de Barcelona 180/2006, seguida con posterioridad por otras varias resoluciones judiciales).

En consecuencia, a la vista de todo lo expuesto, la reforma se ajusta y está en consonancia con los diversos pronunciamientos judiciales dictados al efecto, que tratan de asegurar la proporcionalidad de la pena al beneficio económico obtenido.

Y en segundo lugar, la Ley Orgánica 5/2010, de 22 de junio modifica los apartados 1 y 2 del artículo 274, que quedan redactados como sigue:

> «1. Será castigado con las penas de seis meses a dos años de prisión y multa de doce a veinticuatro meses el que, con fines industriales o comerciales, sin consentimiento del titular de un derecho de propiedad industrial registrado conforme a la legislación de marcas y con conocimiento del registro, reproduzca, imite, modifique o de cualquier otro modo usurpe un signo distintivo idéntico o confundible con aquel, para distinguir los mismos o similares productos, servicios, actividades o establecimientos para los que el derecho de propiedad industrial se encuentre registrado. Igualmente, incurrirán en la misma pena los que importen estos productos.
>
> 2. Las mismas penas se impondrán al que, a sabiendas, posea para su comercialización o ponga en el comercio, productos o servicios con signos distintivos que, de acuerdo con el apartado 1 de este artículo, suponen una infracción de los derechos exclusivos del titular de los mismos, aun cuando se trate de productos importados.
>
> 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 276, el Juez podrá imponer la pena de multa de tres a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días. En los mismos supuestos, cuando el beneficio no exceda de 400 euros, se castigará el hecho como falta del artículo 623.5».

El artículo 274 CPEN se destina a la protección de un importante grupo de derechos de propiedad industrial, los signos distintivos del empresario, de la empresa y de los productos y servicios que sean objeto de la actividad empresarial. Por tanto, el objeto material del delito lo serán las marcas y nombres comerciales. Para la adecuada integración del precepto será necesario acudir a la vigente Ley 17/2001, de 7 de diciembre, de Marcas.

La reforma de 2010, además de introducir algunos ajustes técnicos en determinados conceptos (33), incorporó al apartado 2 un segundo párrafo que es sustancialmente idéntico al nuevo párrafo segundo del apartado 1 del artículo 270, a cuyo comentario nos remitimos.

## 6. Conclusión

Las nuevas tecnologías aplicadas a la delincuencia presentan una serie de aspectos impensables para la delincuencia convencional clásica:

*a)* Se comenten fácilmente.
*b)* Requieren escasos recursos en relación al perjuicio que causan.
*c)* Sus rastros se transforman y pierden con rapidez.
*d)* Pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma.
*e)* Se benefician de las lagunas de punibilidad que pueden existir en determinados Estados.

Estas características obligan a abordar la ciberdelincuencia con nuevas cautelas, técnicas e instrumentos procesales, lo cual determina que las diversas legislaciones penales estén en pleno proceso de adaptación para incluir, en sus tipos penales, aquellas conductas lesivas cometidas por medio de sistemas informáticos o, directamente, cuando están dirigidas a lesionar o poner en peligro su integridad.

Sin entrar aquí en las autorizadas críticas técnicas formuladas a la reforma, esta puede ser calificada de «insuficiente» y, quizás, como operación de *restyling*. El legislador sigue desconociendo la singular importancia que tienen los proveedores de servicios en Internet (ISPs) y los operadores de telecomunicaciones, puesto que cumplen una función indispensable para el correcto funcionamiento del sistema. Sin embargo, el legislador no se ha ocupado suficien-

(33) *Vid*. Manzanares Samaniego, *op. cit*., II, pp. 643 a 645.

temente de sus implicaciones y responsabilidades, ignorando que la amplia factibilidad que ofrece el ciberespacio para la prestación de servicios determina, en cierta medida, una cuota de responsabilidad en el control de los asuntos, objetos o servicios ofrecidos a través de Internet.

Así, ya sea en los supuestos de difusión de un artículo o comentario difamatorio, la oferta de objetos ilegales, el alojamiento o la difusión de una página web cuyo contenido temático es la pornografía infantil, la construcción de un artefacto explosivo o, en fin, la puesta a disposición de contenidos protegidos por los derechos de autor, por citar algunos ejemplos prototípicos, se impone la necesidad de que los proveedores efectúen un *mínimo* control de los contenidos y de los servidores existentes en Internet y que albergan en sus instalaciones (servicios de *hosting* y *housing*). Este es el gran reto que debe recibir una respuesta urgentísima y que la reforma de 2010 no ha acabado de cerrar.

La realidad legislativa nos ha enseñado que dichas modalidades delictivas no siempre pueden ser adecuadamente engarzadas por los tipos penales clásicos, diseñados y redactados para prevenir y reprimir la delincuencia tradicional, y que resultan ajenos a los modernos mecanismos de agresión de bienes jurídicos. La resistencia a la adaptación de los Códigos Penales determina un auge de los ciberdelitos, sirviéndose de la existencia de lagunas de impunidad que deben de ser inmediatamente superadas. En este punto, la reforma de 2010 ha resuelto algunas de ellas, pero es necesario que el Legislador esté en alerta para poder dar una pronta respuesta, pero también prudente y meditada, a los nuevos retos e insuficiencias que se produzcan a partir de la misma.

La presente exposición ha puesto de relieve que la ciberdelincuencia constituye un reto considerable, tanto para los ciudadanos como para los Estados y la Administración de Justicia. Sin embargo, la solución y superación de los problemas, aunque difícil, es posible mediante un concierto de todos los sectores afectados. La protección de la información frente a la «criminalidad del futuro» exige estos esfuerzos. Ya decíamos al principio que el Derecho Penal debe amoldarse a la realidad (y no a la inversa), siendo una de sus funcio-

nes la de canalizar, por cauces adecuados, la nueva realidad social, económica y cultural en que se traducen los avances de Internet.

De este modo, el Derecho Penal y las nuevas tecnologías, a la vista de su uso cotidiano, deben ahora dialogar y estar en permanente conexión para rediseñar los límites y las atribuciones del nuevo espacio jurídico que debe dar respuesta a los retos y desafíos que plantea la Red.

Por ello, cobra especial importancia la adopción de medidas técnicas y preventivas en relación a la seguridad informática. Así, podemos citar la figura del CERT-IT italiano (34), organismo sin ánimo de lucro que realiza actividades de investigación y desarrollo en el campo de la seguridad de los sistemas informáticos y es punto de referencia de las víctimas de intrusiones informáticas en Internet. Ante un incidente informático, la organización identifica el incidente, sugiere acciones para solventar el problema, informa sobre medidas de seguridad y desarrolla programas de control y seguimiento. En España, el Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO) cuenta con INTECO-CERT, cuya finalidad es también servir de apoyo preventivo y reactivo en materia de seguridad en tecnologías de la información y la comunicación tanto a entidades como a ciudadanos. Tiene vocación de servicio público sin ánimo de lucro y ofrece ayuda que, en todos los casos, es gratuita y de rápida gestión. Asimismo, la Policía Nacional y la Guardia Civil cuentan con unidades especializadas en esta clase de delincuencia (la Brigada de Investigación Tecnológica, BIT y el Grupo de Delitos Telemáticos, GTD, respectivamente).

Para concluir, insistiremos una vez más en priorizar este fenómeno que constituye uno de los retos del siglo XXI, como ya analizamos

(34) Se denomina CERT (Computer Emergency Response Team, Equipo de respuesta ante emergencias informáticas) a un conjunto de personas responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. También se puede utilizar el término CSIRT (Computer Security Incident Response Team, Equipo de respuesta ante incidencias de seguridad) para referirse al mismo concepto.

en otra ocasión (35). Incluso hay una corriente doctrinal italiana que considera la llegada un momento en que el ordenador formará parte de la sociedad de tal manera que la delincuencia se realizará a través de medios telemáticos y ya no se hablará de delincuencia informática sino de delincuencia *a secas* (36).

(35) Moisés Barrio Andrés, «Criminalidad e Internet: Retos del Siglo xxi», en *Sentencias de TSJ y AP y otros Tribunales,* núm. 15, Aranzadi, Pamplona, 2003.

(36) Marco Strano, «Nuove tecnologie e nuove forme criminali», en *Cybercrime: conferenza internazionale (La Convenzione del Consiglio d'Europa sulla criminalità informatica)*, Giuffrè Editrice, Milán, 2004, p. 114.