REGULACIÓN PENAL DE LA DELINCUENCIA INFORMÁTICA

Especial referencia a la reforma del Código Penal en materia de ciberdelincuencia tras la Ley Orgánica 1/2015, de 30 de marzo

Universidad de Valladolid

Facultad de Derecho

Alejandro Virumbrales de Rojas

Tutor: Mercedes Alonso Álamo, Catedrática de Derecho Penal

Julio 2015

RESUMEN

El presente trabajo está orientado a establecer cuál es la regulación penal de los principales delitos informáticos que recoge el Código Penal, así como los cambios que ha sufrido como consecuencia de la reforma introducida por la Ley Orgánica 1/2015, de 30 de marzo.

Además, se tratarán los caracteres básicos que componen estos delitos y a los diferentes instrumentos internacionales que afectan a nuestro Derecho interno en dicha materia.

PALABRAS CLAVE

Delitos informáticos; ciberdelitos; Tecnologías de la Información y la Comunicación (TIC´s); Internet; reforma penal; daños informáticos; fraude informático; intimidad; propiedad intelectual; libertad sexual; grooming; ciberacoso; amenazas; injurias; ciberterrorismo.

ABSTRACT

The main goal of this research is to explain the Spanish criminal regulation about cybercrime. Furthermore, in this paper will be studied the changes produced with the last penal reform introduced by the Organic Law 1/2015, of March 30.

Finally, it will be explained the main characters which form these crimes and the international instruments which affect our internal law in the matter.

KEYWORDS

Informatic crime; cybercrime; Information Technology and Communication (ICT); Internet; penal reform; informatics damage; informatics scam; privacy; intellectual property; sexual freedom; grooming; cyber bullying; threats; insults; cyberterrorism.

ÍNDICE DE ABREVIATURAS

AP: Audiencia Provincial.

BOE: Boletín Oficial del Estado.

CC: Código Civil.

CE: Constitución española.

CP: Código Penal.

Dir: Directiva.

ed: Edición.

Ej.: Ejemplo.

LEC: Ley de Enjuiciamiento Civil.

LECrim: Ley de Enjuiciamiento Criminal.

LPI: Ley de Propiedad Intelectual.

LO: Ley Orgánica.

LOPJ: Ley Orgánica del Poder Judicial.

pg: Página.

RD: Real Decreto.

STC: Sentencia del Tribunal Constitucional.

STS: Sentencia del Tribunal Supremo.

ss: Siguientes.

TC: Tribunal Constitucional.

TICs: Tecnologías de la información y la comunicación.

TRLPI: Texto Refundido de la Ley de Propiedad Intelectual.

TS: Tribunal Supremo.

TSJ: Tribunal Superior de Justicia.

UE: Unión Europea.

Vid: Véase.

Vol: Volumen.

ÍNDICE GENERAL

PARTE PRIMERA

INTRODUCCIÓN Y CONCEPTUALIZACIÓN DE LA CIBERDELINCUENCIA

PARTE SEGUNDA

REGULACIÓN PENAL DE LA CIBERDELINCUENCIA

PARTE PRIMERA

INTRODUCCIÓN Y CONCEPTUALIZACIÓN DE LA CIBERDELINCUENCIA

CAPÍTULO I. **APARICIÓN DE LA DELINCUENCIA INFORMÁTICA**

En la actualidad vivimos en una sociedad cada vez más globalizada donde conforme pasan los años y a medida que la economía, la sociedad, la cultura y la tecnología se van desarrollando, los diferentes Estados se van interconectando más entre sí, generando con ello una serie de consecuencia en todos sus niveles.

Desde la política hasta la demografía, la globalización produce que todos los Estados estén cada vez más cerca pudiendo incidir los unos en los otros.

De las diversas causas que motivan este fenómeno destaca la tecnología, que ha venido experimentando un desarrollo en las últimas décadas como consecuencia de los cambios acaecidos en el entorno. Gracias a ella se ha permitido al conjunto de la civilización avanzar de forma exorbitante, pudiendo desarrollar su nivel de vida a un ritmo mucho más rápido de lo que venía siendo posible en los últimos siglos.

Los efectos de lo anterior se ven diariamente con los nuevos mecanismos e instrumentos que hacen de nuestra vida que sea mucho más cómoda y sencilla.

Sin embargo no todo han sido beneficios ya que en los últimos años y como consecuencia del rápido avance de las nuevas tecnologías, se han desarrollado los llamados "ciberdelitos" o delitos informáticos[1], es decir aquellas conductas delictivas derivadas del uso indebido de las nuevas tecnologías que ocasionan perjuicios en bienes jurídicos tanto a escala individual como global, tanto en intereses patrimoniales como no estrictamente

[1]http://www.interior.gob.es/web/interior/prensa/noticias/asset_publisher/GHU8Ap6ztgsg/content/id/2037763

patrimoniales, por ejemplo en forma de estafas mediante páginas web o amenazas en redes sociales respectivamente.

Hay quien a raíz de estos cambios ve en ellos una manifestación más de la Sociedad del riesgo y con ello el Derecho penal del riesgo[2] [3], según el cual como consecuencia de la evolución de la criminalidad es necesario demandar una mayor seguridad a las autoridades.

Según los datos facilitados por el Ministerio del Interior[4], en los últimos años más de 5.000 personas fueron detenidas e imputadas por la comisión de un delito informático, siendo el fraude el principal tipo delictivo cometido, seguido de lejos por las amenazas y coacciones, así como por las injurias y calumnias.

No obstante, el número total de denuncias en esta materia llegó hasta las 50.000, lo que supone un notable incremento si se comparan con las de años anteriores. A pesar de ello, esta cantidad no representa ni el 2% del total de delitos cometidos en nuestro país.

Sin embargo la cifra es relativamente baja, ya que la mayoría de las personas que sufren algún tipo de delito informático no llegan a denunciarlos ante la dificultad de su persecución, debido a la facilidad de los autores para esconderse dentro del mundo virtual. Por ello el número de delitos es bastante mayor de lo que reflejan las estadísticas puesto que además muchas de las personas que los sufren no son conscientes de ello y no consideran tales acciones como constitutivas de delito.

En este sentido destaca una encuesta realizada hace años por el Instituto Nacional de Ciberseguridad[5], en la que se manifiesta que alrededor del 72% de los ordenadores con conexión a Internet contienen algún tipo de *malware*, es decir una clase de virus informático. Sin embargo, y a pesar de que la mayoría de las personas encuestadas estaban siendo objeto

[2] ANARTE BORRALLO, E., "Incidencia de las Nuevas Tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información", en: *Derecho y Conocimiento, Anuario Jurídico sobre la Sociedad de la Información*, Volumen 1, Universidad de Huelva: Facultad de Derecho, 2001, pp: 191 y ss.

[3] Doctrina penal surgida en la sociedad post industrial que explica como al existir tantas conductas que generan riesgos para los bienes jurídicos protegidos por factores difícilmente controlables o evitables, el derecho penal debe pasar a tener un carácter preventivo que trate de contener esos riesgos, centrándose en el llamado "peligro abstracto".

[4]http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815

[5] https://www.incibe.es/

de un ciberataque, al mismo tiempo otorgaban un 76,4% de confianza a Internet, sintiéndose seguras en la red[6].

Con estos datos se ve claramente que en el ámbito de la ciberdelincuencia y a diferencia de otros ámbitos de aplicación del Derecho penal, como los relativos a la integridad física o el patrimonio (una pelea o un hurto por ejemplo), las víctimas no se ven como tales e incluso no son conscientes de la gravedad que representan estos delitos para la sociedad, al ver normal y frecuente su práctica. Es un ámbito muy influenciado por las nuevas tecnologías, que al estar al alcance de todo el mundo y ser usadas de forma generalizada, incluso por niños, no crean la sensación de peligro pues se consideran familiares.

[6] http://www.elmundo.es/navegante/2007/06/20/tecnologia/1182325984.html

CAPÍTULO II. **CONCEPTO, CARACTERES Y CLASES**

Cuando hablamos de delitos informáticos nos referimos a una categoría delictiva que es cometida por medio de un elemento de carácter tecnológico. Es decir, son delitos que cuentan con un elemento informático o tecnológico en su comisión.

No obstante existen también delitos informáticos que no están específicamente pensados para ser cometidos por medio de nuevas tecnologías, como es el caso de las injurias por ejemplo, donde su tipo básico no hace referencia alguna a la informática, derivando del mismo artículo tanto la comisión normal como la cibernética. De esta forma además de la forma tradicional con la que se puede cometer el delito es posible ejecutarlo mediante el uso de las nuevas tecnologías.

Antes de comenzar con el estudio de los tipos penales que forman los ciberdelitos, es necesario hacer una serie de precisiones generales en cuanto a sus características generales[7].

- En primer lugar cabe señalar que a pesar de denominar a estos actos delictivos como *ciberdelitos* o *delitos informáticos*, no todos ellos tienen como forma de ejecución la informática en sentido estricto, es decir los ordenadores o las TICs, (tecnologías de la información y la comunicación), ya que muchos de ellos se pueden cometer mediante otro tipo de instrumentos, como un teléfono móvil por ejemplo. De ahí que haya más de una forma de comisión, no solo mediante un ordenador.

  De ello se deduce la gran dimensión que abarcan estos delitos al englobar dentro de sí una amplia mezcla de comportamientos que tienen como factor común el haberse cometido mediante un instrumento telemático.

- En segundo lugar es importante advertir que en su comisión suelen intervenir dos jurisdicciones, pues en la mayoría de los delitos informáticos al ser cometidos mediante Internet o tecnologías similares ofrecen muchas posibilidades de contactar a distancia con la víctima provocando problemas de ley aplicable[8], en

[7] MIRÓ LLINARES, F., "Cibercrimen y vida diaria en el mundo 2.0. Las teorías del crimen y la oportunidad en ámbitos específicos", 2014, pp.421-443.

[8] GÓMEZ TOMILLO, M., *Responsabilidad Penal y Civil por Delitos Cometidos a través de Internet. Especial consideración del Caso de los Proveedores de Contenidos, Servicios, Acceso y Enlaces,* Aranzadi, Navarra, 2006, pp. 89-91.

relación a si se debe enjuiciar conforme a la ley del país en que el autor desarrolla la conducta ilícita, o a la de la víctima donde se produce el resultado y se consuma el delito.

Con carácter general se viene aplicando la teoría de la ubicuidad que mezcla la posibilidad de atender al lugar en que se ejecutó la acción delictiva y en el que se produjo el resultado. Según esta teoría España sería competente para enjuiciar estos delitos sí ahí fue donde se realizó la actividad antijurídica o se produjo el resultado.

La teoría expuesta debe aplicarse en consonancia con las reglas generales de territorialidad del art.23.1 de la LOPJ[9] y las particulares de los art.14 y ss. de la LECrim.

Esta problemática es muy frecuente en los ciberdelitos al ser Internet un medio que permite conectarse con cualquier parte del mundo al instante. Por ello su persecución e investigación se van haciendo cada vez más complejas, lo que obliga a las Fuerzas de Seguridad a desarrollar nuevos medios de prevención.

- También cabe señalar que los autores de estos delitos no son siempre personas con altos conocimientos de la informática (*hackers* o *crackers* entre otros como veremos más adelante), sino que muchas veces son personas corrientes con acceso a Internet.

  Se trata de un tópico clásico el asociar estos delitos a personas con escasa vida social que pasan mucho tiempo en Internet, pero no es así ya que por ejemplo si un adolescente sube fotos comprometidas de una amiga a una red social sin su permiso, estaría realizando un delito contra la intimidad tipificado en el art.197 CP.

- Además en relación a la autoría importa señalar lo previsto en el art.30 del CP al disponer que *"en los delitos y faltas que se cometan utilizando medios o soportes de difusión mecánicos no responderán criminalmente ni los cómplices ni quienes los hubieren favorecido personal o realmente"*. Es decir que solo los autores podrán ser condenados por la comisión de un ciberdelito, excluye de responsabilidad penal a los cómplices y encubridores.

[9] Téngase en cuenta la reforma operada en el citado artículo por la Ley Orgánica 1/2014, de 13 de marzo, relativa a la justicia universal. Según esta se introducen una serie de requisitos que limitan las competencias de la jurisdicción penal española para enjuiciar delitos cometidos fuera de sus fronteras.

La referencia a los *medios o soportes de difusión mecánicos* debe ser interpretada conforme a un concepto actual que permita vincularlos a los delitos informáticos, ya que de no hacerse así el precepto quedaría vacío de contenido en una sociedad tan tecnológica como la nuestra[10].

A continuación para regular la autoría en estos delitos el Código Penal establece una prelación en función del tipo de autor que sea incriminado, de tal modo que en primer lugar responden quienes hayan redactado el texto o signo por el que se comete el delito; en defecto de estos los directores de la publicación o programa; después los directores de la empresa directora, emisora o difusora; y finalmente los directores de la empresa grabadora, reproductora o impresora.

- En cuanto al resultado que producen tales delitos cabe señalar la amplitud de los comportamientos que se subsumen dentro de sus conductas, pues afectan a bienes jurídicos como la intimidad, la libertad, el honor o el patrimonio entre otros. Siendo en este último caso especialmente perjudicial para la víctima al generar importantes ganancias al autor en detrimento de la víctima que ve rápidamente disminuido su capital.

- También destacan en los ciberdelitos las dificultades en la averiguación y comprobación de los hechos, tanto desde las posibilidades de que los autores sean procesados, como desde la búsqueda de medidas que palien tales hechos, pues es sencillo para los autores ocultarse en la red mediante redes que permiten su encriptación o codificación.

- Finalmente cabe señalar que aunque para ser víctima de un delito informático no es imprescindible un uso abusivo de Internet, la conducta que tenga la víctima va a incidir en el delito ya que existen diversos factores de riesgo que aumentan las posibilidades de ser víctima de ellos, como la visita a páginas de Internet susceptibles de contener virus, la tenencia de cuentas de correo o las descargas que se realizan.

[10] GÓMEZ TOMILLO, M., *Libertad de información y teoría de la codelincuencia. La autoría y la participación en los delitos cometidos a través de los medios de comunicación de masas,* Comares, Granada, 1998, pp. 126 y ss.

Junto al elemento tecnológico de los delitos informáticos, todos ellos tienen en común que no están sistematizados de ninguna forma en el Código Penal, pues se encuentran dispersos por el mismo a lo largo de sus diferentes Títulos de la parte especial. Ello produce que en algunos casos haya que realizar una labor de interpretación cuando el tipo no contemple elementos de carácter tecnológico que permitan su comisión, como sucede en el delito de injurias por ejemplo.

> Además el propio Código Penal hasta la reforma de este año no ha incluido el término "delito informático". Ahora sin embargo en la L.O 1/2015 por lo que se ha modificado, se añade un nuevo artículo 127.bis que menciona por primera vez ese término en relación a los delitos informáticos contra la intimidad y de daños[11].

Para esta tarea sirve de gran ayuda la Instrucción 2/2011[12], dictada por la Fiscalía General del Estado tras la creación en el año 2010 de una plaza especializada de Fiscal de Sala Coordinador en materia de Criminalidad Informática.

La principal ventaja de esta Instrucción es que en ella se contempla una relación de delitos informáticos, facilitando la tarea de interpretación al tener ya clasificados los diferentes delitos con sus modalidades concretas.

La clasificación que recoge la Instrucción se articula en base a 3 criterios:

- En primer lugar los delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos. Aquí encontramos el delito de daños (art.264 y ss. CP); de descubrimiento y revelación de secretos contra particulares o empresas (art.197 y 278 CP); asi como delitos contra los servicios de radiodifusión e interactivos (art.286 CP).

- En segundo lugar los delitos donde la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las nuevas tecnologías, (TICs: tecnologías de la información y la comunicación). En este bloque encajan delitos como el de estafa, (art.248.2 CP); delito de acoso a menores de 13 años, (art.183.ter CP); delitos de corrupción de menores o de personas con discapacidad necesitadas de especial protección; o relativos a pornografía infantil o referida a personas con discapacidad

[11] http://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3439.pdf

[12]https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/memoria2012_vol1_instru_02.pdf?idFile=6311c525-d23a-45d7-9e50-458f6f8c3406

necesitadas de especial protección, (art.189 CP); delitos contra la propiedad intelectual, (art.270 y ss. CP).

- Finalmente aparecen los delitos informáticos donde además de servirse de las tecnologías de la información y la comunicación (TICs) para realizar su ejecución son necesarios conocimientos específicos, como es el caso de la falsificación documental, (art.390 y ss. CP); delitos contra el honor, (art.211 y ss CP); delitos de amenazas y coacciones, (art.169 y ss.); delitos contra la integridad moral, (art.173.1); delitos de apología o incitación a la discriminación, el odio y la violencia, o de negación o justificación de los delitos de genocidio, (art.510 y 607.2 CP).

- Para concluir se añade una cláusula de cierre que incorpora la posibilidad de incluir en esta lista cualquier otro tipo delictivo en cuya ejecución haya sido determinante la utilización de las TICs y en el que dicha circunstancia genere una especial complejidad en la investigación criminal.

  En este sentido destaca la reforma del Código Penal que se ha producido en materia de terrorismo mediante la LO 2/2015[13], de 30 de marzo que tipifica supuestos concretos de ciberterrorismo. La reforma contempla una serie de modificaciones relativas a la captación y adiestramiento de terroristas, incluido el adiestramiento pasivo mediante el uso de las redes de comunicación y tecnologías de la información y la comunicación.

[13] http://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3440.pdf

CAPÍTULO III. **IMPACTO EN EL DERECHO PENAL. FORMAS DE PREVENCIÓN**

La consecuencia de todo lo anterior es la amplitud que abarcan los delitos informáticos constituyendo una forma de criminalidad que a día de hoy se sigue incrementando.

Ello ha provocado un cambio en las Fuerzas y Cuerpos de Seguridad del Estado que han tenido que adaptarse a esta problemática cambiando la forma de perseguir e investigar estos delitos[14]:

- Para ello se han creado nuevas Brigadas especializadas en Investigación Tecnológica y Seguridad Informática dentro del Cuerpo Nacional de Policía[15].

- Dentro de la Guardia Civil se ha creado el Grupo de Delitos Telemáticos[16].

- Y a nivel europeo se ha abordado esta problemática mediante la creación de un Centro Europeo del Cibercrimen que forma parte de la estructura de Europol con sede en la Haya.

A la vez España ha suscrito en 2010 un Convenio sobre Ciberdelincuencia[17] [18].

La ciberdelincuencia es por tanto un ámbito que está en continua expansión y que se ha visto incrementada con la aparición de las nuevas tecnologías, haciendo que todas estas formas de delincuencia se hayan expandido.

Al mismo tiempo el Derecho penal se ha tenido que ir adaptando con la incorporación de nuevos tipos penales como los que aparecen en la LO 1/2015 que reforma el Código Penal tras haber quedado obsoletas ciertas figuras del de 1995.

---

[14] Véase más ampliamente MENDO ESTRELLA, A., "Delitos y Redes Sociales: mecanismos formalizados de lucha y delitos más habituales. El caso de la suplantación de identidad", *Revista General de Derecho Penal 22,* 2014, pp. 2-7.

[15] http://www.policia.es/org_central/judicial/udef/bit_alertas.html

[16] https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

[17] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

[18] Vid. epígrafe II.2.

Para poder realizar esta tarea de adaptación el Derecho penal debe valorar el bien jurídico que es menoscabado en la acción[19] y así enjuiciar su desvalor específico para poderle aparejar una sanción penal.

Junto al Derecho penal debemos tener en cuenta la labor que en este ámbito realiza la Criminología, pues trata de estudiar las causas que determinan las dificultades en la detección de los ciberdelitos, en la identificación de los autores y en la concreción de la ley aplicable, además del perfil de dichos autores[20].

[19] MUÑOZ CONDE, F., GARCÍA ARÁN, M., *Derecho Penal, Parte General,* Tirant lo Blanch, Valencia, 2010, pp. 213-219.

[20] DE LA CUESTA ARZAMENDI, J. L., PÉREZ MACHÍO, A. I., SAN JUAN GUILLÉN, C., "Aproximaciones criminológicas a la realidad de los ciberdelitos"; en: *Derecho penal informático,* Aranzadi, Navarra, 2010, p.84.

PARTE SEGUNDA

REGULACIÓN PENAL DE LA CIBERDELINCUENCIA

Acerca de la sistemática seguida

El contenido de esta parte lo formará el estudio de los diferentes tipos penales que dan lugar a los delitos informáticos, es decir aquellos que se cometen por medio del uso de las nuevas tecnologías.

El orden con el que se tratarán las diferentes figuras delictivas será el que aparece en la Instrucción 2/2011 de la Fiscalía General del Estado anteriormente citada. Esto explica que no responda al criterio del bien jurídico protegido ni a la sistemática del Código Penal.

El motivo obedece a las escasas referencias legales que hay en la materia, siendo dicha Instrucción una de las pocas al respecto, pues el propio Código Penal no contiene prácticamente ninguna al ser los delitos informáticos una categoría doctrinal. De este modo parece lógico seguir el orden que la Fiscalía General del Estado establece para clasificar tales delitos.

CAPÍTULO I. **TIPOS PENALES AFECTADOS POR LA DELINCUENCIA INFORMÁTICA**

SECCIÓN PRIMERA: **DELITO DE DAÑOS Y SABOTAJE INFORMÁTICO**

1. Introducción y cuestiones comunes a los daños informáticos

El delito de daños informáticos o sabotaje informático constituye uno de los principales delitos informáticos al ser una conducta específicamente regulada por el legislador para ser cometida por medio de nuevas tecnologías, pues junto al tipo básico en materia de daños aparecen otros tipos específicos en relación a los daños informáticos.

La regulación del delito de daños se encuentra ubicada en el Capítulo IX del Título XIII del segundo Libro del Código Penal, en los artículos 263 y ss. Sin embargo el desarrollo normativo específico de los daños informáticos lo forman los art.264 más los art.264.bis, ter y quater, añadidos en la última reforma de 2015.

El objeto material de los daños informáticos que se protege en este Capítulo lo forman esas mismas nuevas tecnologías, que son los datos informáticos, los programas informáticos y los documentos electrónicos[21]. E incluso mediante el tipo agravado se otorga protección al sistema informático ajeno de forma global.

1.1 Autoría

Antes de entrar a analizar la regulación penal conviene examinar la figura del sujeto activo en el delito de daños informáticos.

[21] Vid. en este sentido MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Madrid, Edisofer, 2001, pp. 66-67. Por dato el autor entiende a las unidades elementales procesadas por el sistema informático y de cuya combinación resulta la información contenida en el sistema; programas se concibe como las secuencias de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado; y por documentos electrónicos, serian aquellos en los que se recogen los resultados del procesamiento de datos obtenidos con las distintas aplicaciones.

El delito de daños informáticos presenta una singularidad en cuanto a su autoría respecto de la mayoría de delitos informáticos al quedar circunscrita a autores que posean unos conocimientos específicos de la red.

Esta circunstancia no sucede en todos los ciberdelitos, ya que por ejemplo en el de injurias o amenazas la acción no conlleva un carácter altamente informático y elaborado para su comisión sino que basta con el mero acceso a Internet para poder cometer una pluralidad de delitos, como por ejemplo verter difamaciones a alguien en una red social. En cambio en el de sabotaje informático no sucede lo mismo ya que por las propias exigencias de los tipos que le componen, serán necesarias unas habilidades específicas en el manejo de los ordenadores que solo poseerán personas con altos conocimientos de informática.

De esta forma nos encontramos con una triple clasificación respecto de su autoría[22]:

- En primer lugar los ***hackers***, es decir quienes sin autorización acceden a ordenadores o sistemas informáticos en general mediante redes públicas de telefonía o transmisión de datos y con propósitos distintos al de causar un daño, (matiz diferencial con la siguiente categoría de autores). Su fin suele ser el menoscabo de la intimidad de la víctima o la obtención de determinada información que posteriormente no destruyen.

  Además dentro de los *hackers* se encuentran los denominados ***hackers blancos***[23], los cuales no tienen fines destructivos en la red sino que aseguran y protegen los sistemas de Tecnologías de la Información y la Comunicación. Tales sujetos suelen trabajar en empresas de seguridad informática evitando precisamente las conductas delictivas producidas por el delito de daños informáticos.

  También incluidos en los *hackers blancos* se encuentran personas expertas en Internet, que por diversión o curiosidad se dedican a saltar las barreras del sistema descubriendo barreras del mismo, pero sin ocasionar perjuicios a nadie.

[22] Véase más ampliamente GONZÁLEZ RUS, J. J., "Los ilícitos en la red (I): hackers, crackers, ciberpunks, sniffers, denegación de servicio y otros comportamientos semejantes"; en: *El cibercrimen, nuevo retos jurídico-penales, nuevas respuestas político criminales*, Comares, Granada, 2006, pp-241-242.

[23] FERNÁNDEZ TERUELO, J. G., *Cibercrimen, los delitos cometidos a través de Internet,* Constitutio Criminalis Carolina, 2007, p.112.

Finalmente cabe señalar que la figura del *hacker* no solo aparece en el delito de daños, sino también en otros como los del art.197 CP contra la intimidad y de descubrimiento y revelación de secretos. No obstante es en el de daños donde el hacker tiene más repercusión al requerir unos conocimientos informáticos más cualificados de los que se necesitan para cometer otros delitos distintos.

- En segundo lugar los ***crackers***[24], quienes específicamente cometen daños en los sistemas informáticos mediante el acceso o la infección de estos. De manera intencional los *crackers* violan la seguridad de un sistema informático para hacerle daño, eliminar o borrar ficheros, así como introducir algún tipo de virus en él.

  Esta será la figura típica que generalmente revista la autoría en el delito de daños informáticos contemplados en el art.264 y ss. del Código Penal.

- Finalmente encontramos los llamados ***sniffers***, quienes insertan programas en el interior de un sistema informático para introducirse en su disco duro y así poder obtener información. Para ello realizan una técnica denominada *sniffing* que consiste en examinar todos los paquetes de información que van pasando por una red y abrirlos obteniendo contraseñas o información útil para realizar futuras acciones.

1.2 Tipos de ataques a los sistemas informáticos

La clasificación anterior debemos combinarla con las opciones que tienen los distintos sujetos en ella mencionados una vez que se introducen en el sistema informático ajeno.

Las posibilidades quedan circunscritas a dos supuestos:

[24] En este sentido véase MORÓN LERMA, E., *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red,* Aranzadi, Pamplona, 1999, pp.32-33. Para la autora el *cracking* difiere de una conducta análoga para muchos, el ***cyberpunk***, siendo esta última una mezcla entre el *hacker* y el *cracker*, pues consiste en la entrada inconsentida en sistemas informáticos (*hacking)*, pero mediando la corrupción de un *password* (*cracking),* para provocar la destrucción de datos, programas o soportes informáticos, o introducir un virus, una bomba lógica o algo similar. Son conductas similares que comprenden el llamado "vandalismo electrónico" o *ciberpunk*, refiriéndose exclusivamente al daño en Internet y que también encuentran cabida en el art.264 CP. Se vincula a la defraudación de la propiedad intelectual, ya que al dañar el sistema se consigue evitar la protección de los programas informáticos.

- El bloqueo o inutilización, ya sea parcial o total, temporal o definitivo, de páginas web o servicios de Internet.

- La destrucción o alteración, total o parcial de contenidos, información o datos ajenos.

Las dos circunstancias se tratan de igual manera en el derecho español mediante el art.264 CP, ya que lo relevante en nuestro sistema penal es el daño causado.

Tales resultados se conseguirán mediante una serie de acciones realizadas en forma de ataques o accesos no autorizados. Estas acciones por las que se cometen los delitos que serán explicados en esta sección son las siguientes:

- ***Eliminación informática de ficheros***.

  Es la eliminación definitiva de archivos, programas, copias, o incluso la memoria RAM, (siempre que no quede rastro de ello en el sistema). Además tiene que producir un perjuicio mayor que una simple reinstalación ya que debe quedar eliminado por completo.

- ***Introducción en el sistema de virus, gusanos, bombas lógicas, troyanos, bacterias o puertas traseras***.

  Mediante esta conducta delictiva se introducen programas informáticos específicos en el sistema informático que le va destruyendo, tanto a él como a los programas y ficheros que contiene, a la vez que se va propagando a otros sistemas. Se consigue el acceso directo o a distancia al sistema, logrando la destrucción o el daño del mismo.

  Los elementos con que se lleva a cabo están programados para tal fin pudiendo revestir formas muy diversas[25].

  > Entre las opciones con las que se puede dañar el sistema destacan los clásicos **virus**, que son secuencias de códigos insertas en un fichero ejecutable de tal modo que cuando la víctima ejecuta el programa también ejecuta el virus provocando su efecto, que

[25] FERNÁNDEZ TERUELO, J., G., *Cibercrimen, los delitos cometidos a través de Internet,* Constitutio Criminalis Carolina, 2007, p.110-111.

generalmente será la destrucción de archivos que se encuentren almacenados en el entorno del virus.

Por su parte los **troyanos** constituyen programas que simulan ejecutar una función, pero en realidad realizan otra perjudicial para el sistema.

Las **bombas lógicas** son programas como los anteriores, que producen idéntico resultado, pero en este caso se dilata en el tiempo, pues suelen tener una fecha en la que se activa o una cierta secuencia de teclas que debe pulsar la víctima.

Los **gusanos** son programas que se ejecutan y propagan por sí mismos a lo largo del sistema o diferentes redes, portando muchas veces algún tipo de virus.

Las **bacterias** son programas que en sí mismas no dañan al sistema, pero se reproducen ilimitadamente hasta que este se colapsa.

Finalmente las **puertas traseras** son códigos que permiten a quien los conoce acceder a determinados sistemas, programas o información sin tener que realizar los procesos habituales de autenticación.

De este modo la acción tiene muchas variantes debido a que los hackers suelen enmascararla en páginas web, programas o archivos descargables, pero el efecto es el mismo. Sin embargo el delito solo se constituirá cuando sea capaz de destruir, alterar o inutilizar los datos, programas o documentos.

- ***Denegación de servicio***.

Son acciones encaminadas al bloqueo de los equipos mediante el envío de mensajes falsos o gran cantidad de información provocando su colapso y haciendo caer al sistema. No obstante el delito solo quedará constituido cuando la inutilización sea total, no una simple alteración en su funcionamiento.

2. Bien jurídico protegido

El delito de daños como se ha señalado antes se regula en el Capítulo IX del Título XIII del Libro II del Código Penal. Este Título comprende una pluralidad de figuras delictivas que van destinadas a atentar contra el orden socioeconómico en general o el patrimonio de la víctima en particular.

Pero en el delito de daños encontramos que no se sigue esa regla, sino que los tipos que le componen persiguen proteger a la víctima de las conductas que realiza el autor con las que no se enriquece de manera real o posible, sino con las que busca la destrucción o el deterioro de una cosa ajena.

El delito de daños es por ello un delito patrimonial de los denominados "sin enriquecimiento", pues lo que busca es el empobrecimiento ajeno sin que sea necesario el lucro del autor.

Se entiende que las conductas dañosas generan una destrucción de una cosa ajena con independencia del perjuicio patrimonial que ello ocasione a la víctima. De esta forma a diferencia del resto del Título, el patrimonio no es el bien jurídico protegido como tal, pues se atiende al valor de la cosa dañada y no al perjuicio que se genera en el patrimonio de la víctima.

3. Regulación penal

Frente a las anteriores conductas el Derecho penal español ha reaccionado en los últimos años con la creación de nuevos tipos penales. Las reformas son fruto del riesgo que corría el Código Penal de quedar obsoleto ante la aparición de nuevas formas delictivas que generaban situaciones de atipicidad. En tales situaciones, la conducta del autor incorporaba un elemento tecnológico no previsto en el tenor literal del tipo, lo que lo hacía impune por imperativo del principio de legalidad.

De esta forma en el año 2010 con la LO 5/2010[26] se reformó el Código Penal modificando el art.264[27], de tal modo que pasó a regular exclusivamente el delito de daños o sabotaje informático en lugar de ocupar un solo párrafo dentro de ese artículo como venía sucediendo con anterioridad.

Además la materia ha vuelto a ser renovada como apuntábamos antes, pues este mismo año el delito de daños ha sido objeto de modificación con la LO 1/2015, que incorpora al art.264 los art.264.bis, ter y quater. El motivo de la reforma son la multitud de supuestos que comprenden los daños informáticos y que al estar tan relacionados con el

[26] Con anterioridad a 2010 el sabotaje informático quedaba reducido al art.264.2, únicamente a este segundo apartado y no todo el artículo como sucede en la actualidad. La redacción establecía: "*La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".*

[27] http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t13.html

desarrollo de la tecnología hacen que las previsiones del legislador se queden rápidamente obsoletas.

> Antes de entrar con la regulación penal en sentido estricto, cabe precisar que en nuestro sistema jurídico penal no se castiga el mero acceso no autorizado a un sistema informático ajeno. Ello es atípico no constituyendo en sí mismo delito alguno, ya que una vez que el autor se encuentra dentro del sistema se necesita que realice alguna de las finalidades previstas en el tipo orientadas a la destrucción del objeto material. De este modo el mero acceso resulta impune si no va acompañado de actos de ejecución tendentes a producir daños.
>
> Además, las acciones que protegen el sistema informático lo hacen en relación al software, ya que las que atentan contra el hardware son tratadas como un delito de daños del art.263 CP. De ahí que la relevancia en este ámbito la tengan las acciones encaminadas a la destrucción del software, es decir la parte intangible de los sistemas, sus elementos lógicos.

3.1 Tipos penales

El art.264 CP se abre con una previsión general en su primer apartado:

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

El supuesto comprende una serie de conductas tales como borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesible, cuyo resultado es que mediante esos procedimientos no se pueda hacer uso de los datos, programas informáticos o documentos informáticos.

Se habla de un sabotaje más que de un daño para que así la acción no quede reducida al supuesto general del art.263.

Llama la atención que el límite máximo de la pena ha sido aumentado en la última reforma de los dos años de prisión que contemplaba la normativa anterior, a tres.

El tipo exige para su realización que no haya una autorización por parte del propietario del equipo y que el resultado sea grave en relación al valor o patrimonio del sistema.

Para apreciar tal valoración habrá que acudir al valor del mercado, es decir el valor de su venta, o en su lugar a una tasación pericial. En caso de que el objeto del daño no estuviera en el mercado, como sucede en supuestos de archivos o datos que hayan sido

creados por la víctima, se deberá atender al coste de recuperación o de restablecimiento de la información o del sistema, quedando consumado el requisito del daño en caso de que fuera irrecuperable[28].

En este sentido no se debe olvidar que el bien jurídico protegido en estos delitos es el patrimonio. No obstante al valor patrimonial se puede añadir el valor moral del daño como apunta MUÑOZ CONDE[29], que también debe ser susceptible de valoración económica. Además dentro de este valor moral habrá que distinguir entre el daño del objeto material y sentimental, y cuando la distinción no quede clara el autor concluye que "*el perjuicio debe ir referido al daño en el objeto material mismo, independientemente de que otros tipos de perjuicios económicos o morales puedan ser tenidos en cuenta para determinar la pena*".

El segundo número contempla cinco circunstancias agravantes del tipo básico. Las dos primeras ya se preveían en la redacción anterior, siendo novedad por tanto las tres últimas en atención al interés público, que hayan afectado al Estado o a bienes de primera necesidad.

> *"Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:*
>
> - *1.ª Se hubiese cometido en el marco de una organización criminal.*
> - *2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.*
> - *3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.*
> - *4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.*
> - *5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.*
>
> *Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado".*

[28] Véase más ampliamente FERNÁNDEZ TERUELO, J., G., *Cibercrimen, los delitos cometidos a través de Internet,* Constitutio Criminalis Carolina, 2007, p.115-117.

[29] MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, pp 480-481.

Las citadas agravantes tienen en común la especial gravedad que revisten sus conductas en atención al objeto material sobre el que recaen, pues en ellas se alude a servicios públicos, bienes de primera necesidad o incluso a la seguridad del Estado.

Tales conductas cuando se cometan en el entorno de una organización terrorista, darán lugar a la aplicación de sus tipos penales específicos, siendo ello una modalidad diferenciada de ciberdelincuencia que va más allá del delito de daños informáticos o sabotaje informático, pues se trata del ciberterrorismo. A este fenómeno nos referiremos más adelante en el tercer capítulo de esta parte.

El tercer número añade una nueva agravante prevista para castigar los supuestos en los que el autor utiliza datos personales ajenos para ganarse la confianza de un tercero o acceder al sistema informático y ahí cometer el resultado previsto en el tipo básico.

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

Contempla una agravante que entra en relación con los delitos contra la intimidad penados en el art.197 CP, pues para estar ante esta agravante se requiere haber utilizado ilícitamente datos personales de otra persona, lo cual en el entorno informático vendrá por medio de las conductas previstas en el segundo apartado del citado art.197.

Una vez que se obtengan esos datos, para que se consume el delito será necesario que sirvan para introducirse en el sistema que se pretende dañar, o para ganarse la confianza de un tercero.

Por ello es un supuesto que implícitamente se vincula con otros tipos penales y que ha sido añadido en la reforma del pasado mes de marzo, que como venimos señalando modifica bastante esta materia ante el desarrollo de la informática y las nuevas posibilidades que ofrece a los ciberdelincuentes.

A continuación, con la reforma de 2015 se introduce un nuevo art.264.bis que castiga el daño al sistema informático en su conjunto, no al dato, programa o documento que se mantienen como objeto material del tipo básico del art.264.1. De esta forma se separa de una forma más clara el objeto material del delito pues en la anterior redacción la

protección que ahora otorga el art.264.bis al sistema informático en general se hacía en el art.264.2 a continuación del tipo básico, lo que sistemáticamente era más confuso.

> *"Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:*
>
> - *a) realizando alguna de las conductas a que se refiere el artículo anterior;*
> - *b) introduciendo o transmitiendo datos; o*
> - *c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.*
>
> *Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado".*

Ahora tras la reforma introducida por la LO 1/2015 se ha reestructurado el artículo, sistematizándolo a mi juicio mejor de cómo estaba antes, pues el art.264 ha quedado orientado a otorgar una protección básica en la materia, referida a las conductas que atentan contra datos, programas o documentos electrónicos, y que agrava en ciertas circunstancias; y el art.264.bis en cambio se ha situado de forma independiente del anterior para conceder protección a un objeto distinto, más amplio, al que conecta con el tipo básico a la hora de cometerle como se desprende de la letra a), que se vincula con las conductas del art.264.1 referidas al dañado, deterioro, alterado o supresión, pero en este caso del sistema informático.

De este modo las formas de comisión son las mismas que en el tipo básico del art.264.1, pero ahora el resultado es diferente al requerir que afecte a la globalidad del sistema o que provoque su interrupción.

Al igual que sucede en el tipo básico, el resultado debe ser grave en relación al valor o patrimonio del sistema y que el autor actúe sin autorización del propietario del equipo. Los requisitos son idénticos que los expresados más arriba.

No obstante este nuevo artículo trae como novedad otra circunstancia agravante específica para cuando el sistema informático que se daña pertenezca a de una empresa, negocio o de una Administración pública, lo cual provoca un perjuicio mayor al tener una trascendencia económica de mayor importancia pudiendo perturbar su actividad productiva.

Es requisito que el objeto del delito sea el sistema y no el dato, programa informático o documento electrónico del tipo básico, pues el precepto piensa solo en el conjunto del sistema que es lo que ocasiona el verdadero perjuicio a la empresa o Administración, debiendo considerarse en su conjunto y no de forma individual como hace el tipo básico, de ahí que estemos ante una especialidad.

Los dos últimos párrafos del art.264.bis reproducen la fórmula utilizada en el art.264 al remitirse a este último en cuanto a sus agravantes, tanto las del segundo como tercer apartado.

> *"Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior.*
>
> *Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero."*

En estos dos últimos números del art.264.bis se puede apreciar de nuevo la distinción que hace la nueva regulación respecto de los dos objetos materiales que gozan de protección, por un lado los datos, programas y documentos electrónicos, y por otro el sistema informático en su conjunto.

En este sentido el art.264.bis dedicado en exclusiva a la protección del sistema informático se remite al anterior para las cinco agravantes que fueron estudiadas antes, así como a la otra agravante en relación a la obtención de datos personales, que como se señalaba, vendrá en aplicación con el delito comprendido en el art.197.2 CP.

3.2 Caracteres comunes

Las conductas expuestas anteriormente (art.264 y 264.bis) comprenden los supuestos básicos del delito de daños informáticos, difiriendo solo en su objeto material. En su conjunto garantizan una amplia protección frente a todos los daños que sufren los equipos informáticos, ya sea en datos programas o documentos electrónicos.

Sin embargo tales artículos no aluden a las formas de llevar a cabo su ejecución, sino que solo hacen referencia al resultado, es decir la destrucción, alteración o inutilización de los datos, programas o documentos electrónicos. Dentro de tales resultados hay numerosas posibilidades como antes se señalaba ya sea mediante virus, bombas lógicas…

Además es un delito de resultado, es decir que para su consumación no basta con la mera acción sino que requiere un resultado típico. Tal resultado debe haber sido producido por una de las causas que el precepto señala, mediando entre ellos una relación de causalidad.

Respecto a su comisión, puede ser tanto de forma activa como omisiva. Dentro de esta última se niega que una simple omisión pura o simple pueda dar lugar a este delito, pero mediante comisión por omisión sí que podría realizar el delito en casos donde el autor se encuentra en posición de garante respecto del bien jurídico protegido y omite el comportamiento que el ordenamiento espera de él. Por ejemplo el supuesto en que el programador informático de una empresa que se niega a evitar que un virus informático destruya el sistema que tiene obligación de mantener.

En cuanto a la acción, el tipo comprende el borrado, daño, deterioro, alteración, supresión, o inutilización de los datos, programas o documentos. Tales acciones deben conducir a la inutilización del objeto material del delito, que tiene que ser definitiva, de tal forma que cuando el programa no sea eliminado totalmente del sistema o se pueda reinstalar, el tipo quedaría cometido en grado de tentativa.

Cabe también la ejecución del delito en grado de tentativa cuando el resultado no se produce por causas ajenas a la voluntad del autor. Para ello es necesario un comienzo de ejecución previo y la ausencia del resultado por causas no imputables al autor.

En relación a su ánimo subjetivo, se trata de un delito doloso en el que se requiere la voluntad de destruir el elemento lógico o físico del sistema. Además del dolo directo es fácil que concurra el dolo eventual cuando el resultado va más allá del previsto. Es el caso por ejemplo de la persona que crea un virus destructivo pero sin saber si actuará o si quedará latente sin producirse el resultado, al no depender su desarrollo del propio virus.

De manera similar podemos encontrar formas de comisión imprudente, por ejemplo si quien maneja programas susceptibles de dañar el sistema actúa de forma negligente generando un perjuicio en el mismo sin tener esa intención. Este supuesto se contempla en el art.267, que comprende los daños causados por imprudencia grave, siempre que la cuantía del mismo supere los 80.000 euros.

En la modalidad culposa es necesaria la previa denuncia de la persona agraviada o de su representante legal, aunque el Ministerio Fiscal también podrá interponer la denuncia

cuando la víctima sea menor de edad, discapacitada necesitada de especial protección o desvalida.

Finalmente el sujeto activo puede ser tanto una persona física como jurídica, pues mediante la reforma se introduce un nuevo art.264.quater con una previsión para cuando todas las conductas punibles en este ámbito sean cometidas por una persona jurídica.

> *"Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los tres artículos anteriores, se le impondrán las siguientes penas:*
>
> - *a) Multa de dos a cinco años o del quíntuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años.*
> - *b) Multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, 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."*

Esta misma previsión ya se contemplaba en la redacción anterior en el apartado cuarto del art.264.

De este modo la nueva estructura es adecuada, estableciendo ahora un tipo independiente para el hecho de que las personas jurídicas, como sujetos activos del delito, realicen cualquiera de las conductas contempladas en los artículos anteriores.

En conclusión, el estado en que queda la regulación de los daños informáticos tras la citada reforma me parece en su conjunto acertado pues al ampliarse la regulación a más de un artículo, obliga a que las previsiones que estaban solo en un artículo tengan que desplazarse a otros de forma independiente para así abarcar las nuevas conductas punibles, proporcionando más claridad y detalle a la regulación.

Además, de todo lo anterior se desprende que en España el delito de daños informáticos ha ido cobrando importancia con la realización de tres reformas en apenas 15 años. La vinculación de su naturaleza con el desarrollo de las tecnologías y su rápido cambio hace que las conductas que eran inimaginables para el legislador anterior sean perfectamente conocidas para el actual.

4. Creación de virus informáticos. El nuevo art.264.ter

La reforma del pasado 30 de marzo ha introducido en el Código Penal un supuesto específico relacionado con los daños informáticos que hasta ahora era atípico, y con el que se expanden las barreras del Derecho penal de forma considerable.

Se trata del supuesto que contempla el art.264.ter, en el que se castiga a quien crea el programa informático que sirve para producir el delito. Incrimina la mera creación de virus, bombas lógicas o programas similares que tengan la finalidad del art.264.1 o 264.bis.

La peculiaridad es que se castiga a quien crea tales programas aunque posteriormente no se llegue a cometer materialmente el delito, pues basta con la intención de realizarlos más adelante.

> *"Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:*
>
> - *a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o*
> - *b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".*

Se trata de un supuesto en que se castiga a quien crea, adquiere, importa o facilita a terceros tales programas. Contempla una serie de actos preparatorios a la comisión de los delitos que antes se han estudiado.

Es un delito de peligro en el que se adelantan las barreras de protección a estadios anteriores a su realización material. El legislador abandona por ello la fórmula del delito de resultado para incluir dos supuestos que incriminan conductas ajenas al daño en el propio sistema.

No obstante el delito requiere de un especial tipo subjetivo, pues el autor debe llevar a cabo la conducta con la intención de realizar posteriormente alguno de los delitos de los artículos anteriores, el art.264 y 264.bis, es decir los tipos básicos en materia de sabotaje informático.

En este sentido, el autor debe realizar la conducta sabiendo que su intención es la comisión de los delitos del art.264 y 264.bis, de no ser así el tipo sería impune. De este modo en el caso de que alguien por diversión se dedicara a crear o adquirir programas susceptibles de ocasionar daños informáticos, pero que no los usara para producir tal efecto, sino que simplemente experimentara con ellos en su privacidad, la conducta quedaría exenta de responsabilidad penal. Incluso en el caso de que se lo facilitara a un tercero sin saber la ulterior intención delictiva de este, si tal error fuera invencible o vencible, el delito quedaría impune al no estar prevista su comisión culposa.

Junto a las conductas individuales de crear o adquirir el programa o la contraseña, se castiga el hecho de facilitárselo a un tercero, incluyendo por tanto una específica forma de codelincuencia en la materia.

El objeto material del delito, lo que se debe crear, adquirir, importar o facilitar al tercero debe ser un programa informático que sea capaz de producir los delitos de los anteriores artículos, o una contraseña, un código de acceso o algo similar que permite al tercero introducirse en un sistema informático ajeno.

En este sentido el hecho de realizar la conducta de la letra b) daría lugar a un concurso de delitos con el art.197.2, (que posteriormente será tratado en el siguiente epígrafe), pues este artículo castiga a quien se apodere de datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos.

Además, no parece que sea requisito para la consumación del tipo que el futuro delito se lleve a cabo, sino que es suficiente con que pueda llevarse a cabo en el momento en que se le proporciona el programa y el autor tenga esa intención, siendo capaz de producir el resultado de los art.264 y 264.bis.

SECCIÓN SEGUNDA: **DELITOS CONTRA LA INTIMIDAD: DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS; ACCESO SIN AUTORIZACIÓN A DATOS, PROGRAMAS O SISTEMAS INFORMÁTICOS**

1. Introducción

El delito contra la intimidad y de descubrimiento y revelación de secretos es otro de los delitos informáticos clásicos con el que se protege la intimidad de las personas. En este sentido el art.18.1, 18.3 y 18.4 de la Constitución establece:

> *"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
>
> *3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
>
> *4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

El citado precepto de la Constitución está en la base de la actual sensibilidad hacia el derecho jurídico a la intimidad. De esta manera el art.197 del Código Penal incluye una serie de previsiones frente a las conductas tendentes a obtener de forma ilícita secretos documentales, interceptar las telecomunicaciones ajenas o introducirse en los ficheros automatizados.

Tales acciones tienen conexión con los delitos informáticos desde el momento en que para realizar el ilícito el autor se sirve de artificios técnicos, pues como ya se indicó al comienzo de la exposición, los delitos informáticos no son solo los que se cometen mediante un ordenador, sino que es suficiente que lo hagan por medio de cualquier tecnología de la información y de la comunicación, haciendo posible de este modo su comisión por multitud de instrumentos como móviles o cámaras de fotos por ejemplo.

2. Bien jurídico protegido

Con la inclusión del art.197 se consigue que la intimidad figure por primera vez en un Código Penal al hablar explícitamente el Título X de "delitos contra la intimidad",

además de mencionar la propia imagen y la inviolabilidad del domicilio. Todos ellos son bienes jurídicos protegidos en el art.18 CE contra los que este delito atenta.

Se trata de proteger la intimidad junto con los datos reservados de carácter personal o familiar a los que alude el art.197.2 CP.

En este ámbito incide el principio de intervención mínima del Derecho penal, ya que solo se pueden tipificar los ataques que más enérgicamente vulneren los bienes jurídicos protegidos.

> En primer lugar se protege la **intimidad**. Este concepto es difícil de delimitar al estar presente en muchas vertientes de la vida cotidiana y del Derecho, incluso en la actualidad donde con el incremento de los nuevos mecanismos que permiten captar y transmitir la imagen y el sonido se ha hecho mucho más fácil vulnerarla[30].
>
> En este ámbito entran en conflicto diferentes intereses puesto que por un lado desde la esfera estatal se persigue controlar y regular la intimidad, ya que en último término aparece protegida en la Constitución. En cambio desde entornos privados se pide una mayor flexibilidad en dicha regulación para poder llevar a cabo mejor sus actividades, como sucede por ejemplo en el sector del periodismo.
>
> A todo ello se añade el fenómeno de Internet, donde el término "intimidad" es lo opuesto a su esencia ya que todo lo que se desarrolla dentro de él deja una huella permanente muy difícil de borrar. Junto a esto, Internet es un instrumento necesario por el que pasan todas nuestras comunicaciones diarias lo que genera una fuente delictiva enorme en el ámbito de los delitos contra la intimidad.
>
> Como consecuencia de lo anterior se concibe a la intimidad como un derecho inherente de la personalidad, fundamental, estando incluso reconocida a nivel supranacional dentro del Convenio Universal de Derecho Humanos.
>
> Es un derecho que está siendo modulado continuamente mediante las decisiones del Tribunal Constitucional, siendo difícil por ello otorgarle un concepto, aunque en la actualidad tiende a definirse como *el espacio de la vida privada de la persona y las facultades de decisión y de acción del individuo en su esfera privada que permanecen ajenas a cualquier intromisión o limitación por parte de terceros*[31].

[30] Véase más ampliamente ROMEO CASABONA, C. M., "Los datos de carácter personal como bienes jurídicos penalmente protegidos"; *en: El cibercrimen, nuevos retos jurídico penales, nuevas respuestas político criminales,* Ed. Comares, Granada, 2006, pp. 181 y ss.

[31] STC 134/1999, de 15 de julio F.J 5.

En sentido negativo se entiende que con la intimidad se pretende conseguir la *exclusión de terceros de las manifestaciones de la personalidad individual o familiar sin que personas ajenas a su titular puedan tomar parte de ello*.

Además del sentido negativo anterior se encuentra otro positivo que concibe la intimidad como un *derecho de control sobre la información y los datos de la propia persona, incluso de conocidos y que así solo se utilicen conforme a la voluntad de su titular*[32].

Todo ello hace de él como uno de los derechos de la personalidad más sutiles y más difíciles de determinar y proteger por el Derecho penal. Además la intimidad nunca había tenido un reconocimiento autónomo hasta el Código Penal de 1995 junto con la previsión constitucional de 1978[33].

En segundo lugar el Código Penal también se centra en la **protección de los datos de carácter personal** reconocidos en el cuarto apartado del art.18 CE.

Este apartado relaciona el derecho a la intimidad con la informática, dando lugar a un nuevo derecho fundamental que incluye todos los datos de carácter personal introducidos en un sistema informático. Se vincula con la libertad informática donde *el libre desarrollo de la personalidad en una sociedad moderna no queda protegido con la referencia genérica a la intimidad sino que hay que ir más allá siendo necesario este derecho específico a la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitadas de los datos concernientes a la persona*[34].

Todo ello ha dado como resultado la creación del derecho fundamental a la protección de datos personales, y con ello dispensar protección a la recogida, obtención y uso que se dé a este tipo de datos. Se permite decidir al individuo qué información de carácter personal puede ceder a un tercero y cual debe quedar en el ámbito interno, permitiendo así que se oponga al uso por parte de otros.

El último bien jurídico que se incluye en el art.197 es la garantía frente a la **intervención de las comunicaciones privadas**. Esto es respecto a las vulneraciones que se producen mediante artificios técnicos ajenos a quienes participan en la comunicación.

Se trata de otro bien jurídico que se menoscaba mediante la interceptación del mensaje concreto o con el simple conocimiento del mismo. Esta conducta se ha ido extendiendo al ámbito de las nuevas tecnologías al ser cada vez más frecuente que la intromisión se lleve a

[32] STC 254/1993

[33] MUÑOZ CONDE, F., *Derecho Penal parte especial,* Tirant lo Blanch, Valencia, 2010, pp 270-271.

[34] STC 254/1993, de 20 de julio. ROMEO CASABONA, C. M., "Los datos de carácter personal como bienes jurídicos penalmente protegidos"; *en: El cibercrimen, nuevos retos jurídico penales, nuevas respuestas político criminales,* Comares, Granada, 2006, p. 181.

> cabo mediante artificios técnicos que van apareciendo en el mercado, distintos de los propios ordenadores[35].

3. Regulación penal. Tipos básicos

Tras la protección constitucional de la intimidad en el art.18, el Código Penal ha reaccionado incluyendo una serie de tipos en su Título X del Libro II. En ellos se da cabida a la protección penal de la intimidad, a los datos personales y a las comunicaciones ajenas. Además incluye otros bienes jurídicos que no se encuentran en conexión directa con los ciberdelitos al no requerir para su comisión un uso más determinante de las tecnologías de la información y la comunicación.

El desarrollo legislativo de dichos bienes encuentra cabida en el art.197 a lo largo de sus siete apartados, más los nuevos artículos introducidos por la LO 1/2015, 197.bis, ter, quater y quinquies[36].

En ellos se regulan los cuatro supuestos básicos que están en estrecha conexión con los tres bienes jurídicos expuestos anteriormente, así como sus agravantes comunes y conductas singulares que a continuación se expondrán. Además todos ellos son susceptibles de ser cometidos mediante artificios técnicos, e incluso en algunos esta será la única forma posible para realizar la conducta.

Las conductas básicas que se castigan en los dos primeros apartados del art.197 y en el art.197.bis por vulnerar alguno de los citados bienes jurídicos son, en primer lugar las relativas a los secretos documentales; en segundo lugar a la interceptación de las comunicaciones; seguidamente al descubrimiento del secreto informático; y finalmente al acceso a datos y sistemas informáticos[37].

3.1. Secretos documentales

El art.197 se abre con una protección relativa a los secretos documentales al tipificar:

> *"El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales".*

[35] STC 70/2002 de 3 de abril
[36] http://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3439.pdf
[37] MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, pp. 273-280.

Se incrimina a quien se apodera de cartas, papeles, correos o cualquier otro efecto personal que sea susceptible de vulnerar su intimidad. Aquí el bien jurídico protegido es la intimidad, en ningún caso la propiedad ya que el titular no queda desposeído de lo apoderado.

Para que el citado tipo sea de aplicación es necesario que concurra el apoderamiento, es decir que el objeto material se sustraiga de la disponibilidad del propietario quedando a disposición del autor.

De la forma de comisión no se habla en el precepto, dejándola abierta, por lo que cabría la posibilidad de cometer el delito en grado de tentativa. Esto podría suceder por ejemplo en el caso que alguien se apodere de un mensaje sin llegar a leerlo.

Además el tipo solo puede ser cometido por particulares ya que los funcionarios tienen sus previsiones específicas en los art.598 y ss.

Es un delito eminentemente doloso que requiere ese especial injusto. Y para su consumación es preciso que junto con el apoderamiento del objeto material, este quede a disposición del autor de tal forma que la simple lectura de un mensaje ajeno no entraría en esta primera conducta, aunque podría hacerlo en la siguiente. Sin embargo aunque el contenido de lo obtenido no atentara en sí mismo contra la intimidad de la víctima, el tipo seguiría estando cometido ya que el delito se consuma con el mero apoderamiento[38].

Se trata de un delito de peligro y aunque desde un punto de vista teórico el autor debe actuar con tal intención, no es necesario el menoscabo real puesto que en caso de que el contenido se difunda ya está contemplado en su apartado cuarto.

Finalmente la pena prevista para esta conducta es de prisión de uno a cuatro años y multa de doce a veinticuatro meses. La misma que para la interceptación de comunicación como a continuación se detalla.

3.2 Interceptación de comunicaciones

En el segundo inciso del mismo apartado primero se regula la interceptación de comunicaciones.

> *"O intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación".*

[38] MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal,* Edisofer, Madrid, 2001, p. 129.

De nuevo la intimidad queda protegida pero ahora lo hace en relación a las comunicaciones personales y la propia imagen, art.18.1 y 18.3 CE.

Con esta conducta no se perturba o limita la comunicación ajena, sino que el autor se introduce ilegítimamente para conocer el contenido mediante algún tipo de soporte informático.

A diferencia de la conducta anterior sí que se establece la forma de comisión al hablar de artíficos técnicos de escucha, trasmisión, grabación o reproducción. Por tanto queda circunscrito al ámbito natural de aplicación de los delitos informáticos.

El tipo introduce una cláusula abierta al incluir la posibilidad de que sea cometido mediante cualquier otra señal de comunicación. No obstante a pesar ello lo que sí se requiere es que haya un mecanismo o artificio que haga posible la vulneración de la intimidad, un instrumental acorde a la finalidad[39].

Además la conducta debe ser dolosa y el delito se consuma en el momento en que se obtiene la comunicación concreta, el sonido o la imagen. De esta forma el momento en que debe producirse la interceptación de la comunicación debe ser cuando se está produciendo ya que el tipo habla de interceptarla, pues si ya se hubiera producido y estuviera almacenada se aplicarían otros supuestos contemplados en este mismo artículo.

Al igual que en el supuesto anterior la mera interceptación es constitutiva de delito independientemente de lo obtenido, se consuma con la mera interceptación sin que se requiera una difusión. Si la hubiera habría un concurso con el supuesto específico relativo a su difusión.

La pena prevista es la misma que para el supuesto anterior, de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

3.3 Secreto informático

Las conductas orientadas a proteger el secreto informático se contemplan en el segundo apartado del art.197.

[39] De ahí que como señala MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, p.131. El hecho de escuchar una conversación detrás de una puerta constituiría un supuesto atípico para el derecho penal, derivado de las exigencias del principio de intervención mínima.

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

En este precepto a diferencia del anterior no se protege como tal la intimidad como bien jurídico, pues no se habla de cartas, mensajes o similares en abstracto sino solo de datos de carácter personal o familiar que estén registrados en soportes informáticos. En definitiva, el bien jurídico protegido es otro, "datos reservados de carácter personal, familiar u otro", que constituye al mismo tiempo el objeto material sobre el que recae la conducta delictiva.

Ello implica la necesidad de analizar a que se refiere la ley con el adjetivo *reservado,* lo cual conforme a las teorías dominantes[40] [41] serían todos aquellos datos salvo los que estén a disposición de cualquiera.

Cuando hablamos de datos reservados no los podemos circunscribir a determinadas categorías porque para ello el propio art.197 prevé una agravante en su número quinto[42].

El tipo incluye dos formas de comisión, en un primer momento tipifica el mero apoderamiento, utilización o modificación y después el acceso, utilización o alteración. Ambas fases son independientes siendo constitutivas de delito cualquiera de ellas por separado, aunque en realidad es el acceso lo que difiere entre ambas.

Respecto al acceso, aparece mencionado en el último inciso del párrafo, con ello se va más allá de las previsiones anteriores que solo requerían el apoderamiento o uso. Ahora el mero acceso constituiría el tipo, por ejemplo en el caso de que alguien entrara en un ordenador ajeno a ver información aunque después no la utilizara.

Todas estas conductas habrá que ponerlas en relación con los demás apartados del artículo en función del modo que ha tenido el autor de acceder, si ha evitado las medidas de seguridad, el tipo de datos que ha obtenido o si los ha difundido con posterioridad.

---

[40] MARCHENA GÓMEZ, M., "Intimidad e informática: la protección jurisdiccional del habeas data". *Boletín de información. Ministerio de Justicia e Interior* nº 1768, (1996), p.752.

[41] MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, p. 134.

[42] Estos datos reservados podrían coincidir con los que la Ley Orgánica de Protección de Datos, 15/1999 de 13 de diciembre enumera en su art.7 (especialmente protegidos) pero para ello ya está el agravante del art.197.5.

Además al igual que en las conductas anteriores también se requiere el dolo, ya que se tiene que actuar en perjuicio de un tercero o del titular de los datos. No obstante al no ser necesario que el resultado se produzca para que surja la responsabilidad penal por la acción, cabría la posibilidad de cometer el delito en grado de tentativa, (dejando al margen las posibles actuaciones que no fueran idóneas para lograr el resultado que quedan fuera del ámbito penal).

En todo caso se consuma cuando se accede al fichero donde se encuentren los datos y no en fases anteriores.

3.4 Acceso, facilitación o mantenimiento a sistemas de información

El acceso a datos y sistemas informáticos es la última modalidad de comisión delictiva básica que se contempla en el art.197.bis[43] con la siguiente redacción:

> *"El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".*

El supuesto forma la cuarta conducta básica de los delitos informáticos contra la intimidad pero que tras la reforma introducida por la LO 1/2015 ha pasado a ocupar el art.197.bis en lugar del tercer apartado del art.197 como venía haciendo[44].

El objeto material es más amplio que en las conductas anteriores al tratarse de "*el conjunto o una parte de un sistema de información"*. Evoca al que se contempla en el delito de daños informáticos en el art.264.bis, lo cual generaría un concurso de delitos entre ambos preceptos si al realizar la vulneración de la intimidad se generan daños en dicho objeto.

---

[43] Con anterioridad a la reforma tal conducta se regulaba en el art.197.3 CP con una redacción muy similar a la actual, decía *"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 (…)".*
Tal previsión se introdujo por primera vez en la reforma del año 2010 al mantener la protección a los bienes jurídicos señalados pero introduciendo un matiz más acorde a los delitos informáticos al regular específicamente el acceso o mantenimiento dentro de los datos, programas o sistemas informáticos habiendo vulnerado la seguridad.

[44] La reforma es acertada, pues desde un punto de vista sistemático es mejor que este supuesto se regule de forma independiente a las conductas anteriores al presentar unas características singulares acorde a su especial forma de comisión relacionada más específicamente con la ciberdelincuencia a sistemas informáticos, pues las anteriores podía cometerse de una forma más amplia.

El supuesto afecta a la privacidad de los sistemas informáticos para los casos en que el autor acceda o facilite las conductas anteriores.

Lo que se incrimina es el acceso y el mantenimiento, es decir siempre tiene que haber un acceso para estar ante este tipo y luego puede haber o no un mantenimiento. Además de ello con la reforma se castiga el facilitar a un tercero dicho acceso, contemplando de ese modo un supuesto específico de codelincuencia.

El tipo penal queda muy vinculado con las conductas anteriores ya que para su comisión se necesita vulnerar las medidas de seguridad y así entrar en el sistema informático. De no haber tal vulneración estaríamos ante el supuesto segundo del art.197.

Junto a la anterior conducta la reforma ha añadido un segundo número en el art.197.bis estrechamente vinculado con el fenómeno de la ciberdelincuencia. Se trata de la conducta de quien intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información en los siguientes términos:

> *"El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses".*

Se trata de un supuesto específico de interceptación de comunicaciones ajenas, relacionado con la segunda conducta del art.197.1, solo que en este caso se habla de interceptar datos informáticos que estén en un sistema de información, a lo que añade novedosamente las emisiones electromagnéticas.

Finalmente cabe señalar que todas las conductas anteriores son también punibles cuando sean realizadas por una persona jurídica, pues desde la reforma del año 2010 se introdujo en nuestro ordenamiento su responsabilidad penal. De este modo actualmente se contempla una previsión específica en el art.197.quinquies para cuando cometan alguno de los delitos contemplados en el art.197, 197.bis y 197.ter:

> *"Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. (…)".*

En la redacción anterior el supuesto se preveía en el segundo párrafo del tercer apartado del art.197, a continuación de las conductas básicas. Al haber extraído la última conducta relativa al acceso o mantenimiento en sistemas de información ha habido que desplazar tal previsión sobre la autoría de las personas jurídicas. Ello produce sin embargo un efecto global que hace más sencilla la comprensión del ámbito de protección penal de la intimidad, pues al haber ampliado los artículos en esta materia se dota de unidad con uno propio el supuesto de que una persona jurídica sea sujeto activo de cualquiera de los delitos que ahí figuran.

4. Otros tipos penales previstos en el art.197. Especial consideración de la difusión de material obtenido con el consentimiento de la víctima

A continuación de los tipos básicos, el art.197 contempla una serie de tipos cualificados y conductas comunes a las anteriores.

En primer lugar el tercer apartado en su primer párrafo establece una cualificación de la responsabilidad en atención a la divulgación de lo obtenido para los casos en que los autores difundan, revelen o cedan el resultado de las conductas básicas.

> *"Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores".*

En este caso el autor además de cometer el delito básico mediante una de sus cuatro conductas, posteriormente lo que ha obtenido lo difunde, aplicándose la citada agravante. Por tanto se aplican las mismas exigencias que en las anteriores conductas, ya que ellas en sí mismas serán delito pero cuando se divulgue lo obtenido se aplicará este párrafo, pues es autónomo al contemplar un marco normativo propio con independencia de lo anterior.

Cuando esta difusión sea realizada por un tercero ajeno al descubrimiento, pero consciente del origen ilícito del objeto difundido, el segundo párrafo del mismo número también le incrimina. Por ello no es condición imprescindible haber sido el autor de la intromisión ilegítima en la intimidad ajena para ser castigado por ella.

> *"Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior".*

La conducta del tercero debe ser dolosa, pues el párrafo prevé que el autor sepa que el material que está difundiendo ha sido obtenido de manera ilegal. Por tanto cuando no lo supiera o no pudiera haberlo sabido, (es decir que esté ante un error vencible o invencible), la conducta sería impune, al no estar prevista la comisión culposa en ninguno de los casos de este capítulo.

De esta forma se comete el delito tanto si la difusión viene del autor como de un tercero.

Dicha situación plantea problemas prácticos cuando es la víctima quien voluntariamente cede a otra persona imágenes, vídeos, mensajes… quien posteriormente procede a difundirlo.

Con la legislación anterior esta conducta era atípica por muy reprochable que pudiera parecer, (por ejemplo cuando el material difundido contenía relaciones sexuales entre el autor y la víctima), ya que como se acaba de ver la difusión solo estaba penada cuando era consecuencia de la realización de una de las cuatro conductas antes explicadas, es decir que el material hubiera llegado sin consentimiento de la víctima a la persona que lo difunde. De ahí que cuando la víctima hubiera consentido la difusión y posteriormente la persona a quien se lo envía procede a difundirlo la conducta era impune.

El problema desaparece con la reforma de este año al dar una nueva redacción al art.197.7 que permite incriminar a quien difunde imágenes o grabaciones que se han obtenido con consentimiento de la víctima.

El nuevo párrafo séptimo comprende el supuesto en que una persona permita a otra la grabación de vídeos o realización de fotos de ciertos actos pero no su difusión. Además se agrava cuando estos hechos los realiza una persona vinculada a la víctima por su especial relación de afectividad, ya sea presente o pasada.

> *"Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.*
>
> *La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa".*

Esta previsión es una novedad que facilita el encaje judicial de tales situaciones ya que con la anterior legislación al haber un previo consentimiento por parte de la víctima, la posterior difusión no sería delictiva, pues la norma requería que no le hubiera en el momento del apoderamiento.

De esta forma el nuevo párrafo permite unificar en un mismo supuesto los casos en que hay consentimiento para la obtención de imágenes o vídeos pero no para su difusión.

> Es un problema y una realidad de parejas que mientras están juntas se realizan fotos y videos de contenido sexual habiendo consentido ambas personas y tras su ruptura una de las dos lo cede a terceros o lo incluye en redes sociales. Esta tendencia es conocida como ***sexting***[45] y que incluso según el actual art.197.3 CP es atípico, al requerir que no haya habido consentimiento de la víctima a la hora de obtenerle.
>
> De esa manera supuestos donde una persona consiente que la graben y luego el vídeo se difunde, quedaban impunes por muy reprobable que sea la conducta.
>
> Ejemplos de todo ello encontramos en la sentencia de Audiencia Provincial de Alicante de 2 de febrero de 2012 en apelación de los Juzgados de lo Penal como consecuencia de un hombre que fue denunciado tras subir fotos de su pareja semidesnuda a una red social tras haber roto con ella.
>
> Precisamente como consecuencia de estos casos en el propio art.197.7 se ha introducido un segundo párrafo para cuando entre autor y víctima haya o haya habido una análoga relación de afectividad.
>
> De este modo con el nuevo artículo se solucionan estos problemas dando cobertura a muchas situaciones en que el autor se aprovecha de la confianza que tiene o tuvo con la víctima y que le permitió hacerse con material susceptible de vulnerar su intimidad sin que ella pusiera oposición.

El número cuarto de este art.197 establece una agravante en función de si el autor es el encargado o responsable del soporte donde se guardan los objetos materiales del delito y si se han utilizado datos personales del sujeto pasivo.

> *"Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:*
>
> > *a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o*

[45] MENDO ESTRELLA, A., "Delitos y Redes Sociales: mecanismos formalizados de lucha y delitos más habituales. El caso de la suplantación de identidad", *Revista General de Derecho Penal,* 2014, pp. 22-26.

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior".

Además agrava a su vez la responsabilidad si tales datos se han distribuido a terceras personas, provocando un perjuicio mayor a la víctima al tener una mayor repercusión.

La siguiente agravante contemplada en el número quinto es en función del carácter sensible del tipo de datos obtenidos de la víctima. En ella se establece una lista de datos concretos como la ideología, raza o religión, que al constituir aspectos muy vinculados a la personalidad forman el núcleo duro de la intimidad de la víctima.

"Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior".

El número sexto agrava la conducta en atención a la especial finalidad lucrativa por la que se llevan a cabo estos actos. A su vez lo cualifica si la conducta realizada con finalidad lucrativa versa sobre los datos sensibles del apartado anterior.

"Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años".

Finalmente la última agravante la encontramos en el art.197.quater para cuando cualquiera de los hechos penados en el capítulo sean cometidos por una organización o grupo criminal.

"Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.".

Este supuesto le introdujo por primera vez la LO 5/2010 en el apartado octavo del art.197. Sin embargo como consecuencia de la reforma de 2015, al ampliar el artículo añadiendo cuatro nuevos preceptos ha sido necesario sacarle del art.197 para darle uno con autonomía propia y que afecte a toda la regulación en el ámbito de la intimidad. Sucede algo similar que lo que ocurría con la previsión acerca de las personas jurídicas cuando sean sujetos activos del delito.

Además todos los supuestos del art.197 son susceptibles de ser agravados en sí mismos según el art.198 si la acción es realizada por un funcionario público o autoridad, siempre que la ley no se lo permitiese o no estuviera autorizado y además se prevaliera de su cargo[46].

5. El nuevo art.197.ter y los programas informáticos o contraseñas que facilitan la comisión de delitos contra la intimidad

Fruto de la reforma de 2015 se ha añadido el art.197.ter que contempla uno de los pocos supuestos nuevos que trae en esta materia, pues la mayoría de los cambios que contempla son reestructuraciones de tipos ya existentes, alteraciones de penas o introducción de pequeños incisos.

Se trata de un artículo nuevo que castiga una situación atípica por completo hasta ahora, la de la persona que crea programas informáticos o proporciona contraseñas o códigos que permiten y facilitan llevar a cabo los delitos de los art.197.1, 2 y 197.bis, (las conductas básicas), aunque quienes los creen no formen parte de la realización del acto ilícito.

> *"Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:*
>
> *a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o*
>
> *b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".*

La conducta es la de quien crea, produce, usa o importa programas informáticos que sirven para cometer los delitos contemplados en los tipos básicos de los art.197 y 197.bis. Son programas que permiten al usuario acceder a sistemas informáticos ajenos para apoderarse de su información o realizar el resto de conductas penadas en tales artículos, como la utilización de datos personales.

[46] Este supuesto conviene distinguirlo del art.534 a 536 para cuando tal sujeto esté autorizado pero se extralimite en sus funciones

Además se castiga a quien en lugar de realizar el ilícito por medio de programas informáticos obtiene contraseñas o códigos que tienen la misma finalidad de entrar en sistemas informáticos ajenos para ahí desarrollar la actividad delictiva. De este modo una conducta aparentemente inofensiva como desbloquear las contraseñas Wifi del vecino por medio de aplicaciones informáticas sería un delito.

Junto a las conductas anteriores que hacen referencia a un único sujeto, (es decir quién adquiere el programa o contraseña, produce, importa o crea), el tipo contempla la de quien facilita a un tercero cualquiera de esos medios por los que se comete el delito, estableciendo de este modo un supuesto especial de codelincuencia.

Esta previsión relativa al tercero se asemeja a la del art.264.ter para quien facilita a terceros programas capaces de producir daños informáticos. Además no se descarta la aplicación de ambos tipos a la vez mediante un concurso de delitos cuando el autor se introduzca en el sistema informático ajeno a través del programa facilitado y genere daños en los términos que el art.264 exige.

Es preciso que el autor actúe con dolo, es decir con ánimo de vulnerar la intimidad ajena por medio del programa o la contraseña facilitada, pues el propio artículo requiere la intención de facilitar la comisión de los art.197 y 197.bis por medio de tales medios.

En general se trata de un supuesto con el que se expanden las barreras de protección penal a conductas anteriores a la vulneración de la intimidad pero que son susceptibles de lesionarla al hacer más sencilla la comisión de ulteriores delitos.

6. Revelación de secretos de empresa a través de Internet

Íntimamente ligado a los delitos contra la intimidad encontramos el delito de espionaje industrial o de revelación de secretos de empresa tipificado en el art.278 CP.

> *"El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses".*

El artículo está bastante vinculado al supuesto del art.197 pues castiga la conducta de quien se apodera por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos… Es necesario que se produzca el apoderamiento como forma de

realizar la acción, que será llevado a cabo en los mismos términos que los descritos en el art.197.

En este caso solo se incrimina el apoderamiento, no se alude a otras conductas como sí lo hacia el art.197, (la interceptación de comunicaciones por ejemplo), pero al referirse el precepto a quien se apodere *por cualquier medio*¸ parece englobarlo dejando libertad al autor para que lleve la conducta como crea oportuno. Además el propio precepto se remite al art.197 en cuanto a los medios o instrumentos que en él figuran para realizar la conducta.

El apoderamiento puede ser llevado a cabo por cualquier medio como indica el precepto, es decir que no solo se realiza la acción cuando el autor obtiene física o virtualmente la información, sino que bastaría con acceder a la fuente y obtenerla de forma visual o mental.

De lo que se trata es de proteger el secreto de empresa frente al espionaje industrial, que es entendido como el conocimiento reservado a un número limitado de personas y oculto a otras, sobre ideas, productos o procedimientos de valor competitivo para la empresa[47]. Es información sensible y estratégica de la empresa que de llegar a conocimiento de la competencia podría dañar su productividad, volumen de negocios… Se debe tratar de información confidencial y exclusiva pues en definitiva lo que se vulnera es la libre competencia, o la competencia leal entre empresas.

Además el secreto de empresa se entiende de forma amplia, no incluyendo solo los secretos puramente industriales sino también los comerciales u organizativos, como campañas publicitarias o listas de clientes[48].

Cuando dicha acción sea cometida por medio de Internet, la conducta será constitutiva de un delito informático. Además en este sentido la conducta será llevada a cabo en el entorno del *hacking,* es decir de un *hacker* cuyo trabajo es introducirse en las empresas para obtener información sensible. De este modo será frecuente que junto con el delito del art.278 se produzca otro de sabotaje informático del art.264. En este sentido el propio art.278.3 prevé una cláusula concursal específica que señala que las penas en él

[47] FERNÁNDEZ TERUELO, J., G., *Cibercrimen, los delitos cometidos a través de Internet*, Constitutio Criminalis Carolina, 2007, p. 147.
[48] MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, p. 506.

impuestas son sin perjuicio de las que correspondan por la destrucción o apoderamiento de los datos.

Se trata de un delito de peligro al no ser necesario que la información que se obtenga esté dentro de la considerada como "secreto de empresa", pues lo único que se necesita es llevar a cabo la conducta con la intención de encontrarla. En este sentido será necesario que el autor actúe con dolo directo, tanto de apoderarse de dicha información como de descubrirla.

Asimismo el delito se consuma en el momento del apoderamiento, pues si posteriormente la conducta se difunde o revela a terceros entra el juego la agravante del art.278.2 CP.

En el art.279 se incluye otra agravante cuando la conducta sea realizada por quien tenga legal o contractualmente la obligación de guardar reserva. En este caso no concurrirá el apoderamiento al estar el autor legitimado para estar en posesión del secreto de empresa, pero al mismo tiempo tiene la obligación de no revelarla, lo que le convierte en sujeto activo de esta modalidad específica del delito. Para ello dicho sujeto debe saber que lo que conoce forma parte del secreto de empresa y que lo haga por razón de su puesto.

Finalmente la regulación de este delito se cierra en el art.280 al castigar la conducta de quien realice las conductas anteriores sin haber tomado parte en su descubrimiento pero sabiendo su origen ilícito. Se trata de un supuesto similar al del art.197.3 que incrimina las conductas de quienes reciben la información sin haber participado en el descubrimiento y se aprovechan de ella. Por ello será necesario que no hayan participado en su obtención (pues se les aplicaría el tipo básico) y que concurra el específico tipo subjetivo, es decir que sepan que la información fue obtenida de manera ilícita.

SECCIÓN TERCERA: **DELITO DE ESTAFA**

1. Introducción. Aspectos comunes al delito de estafa

1.1 Concepto de estafa para el Derecho penal. Elementos que forman la conducta. El engaño

El delito de estafa constituye otra manifestación de la criminalidad informática, configurándose en la actualidad como la principal expresión delictiva de la ciberdelincuencia en materia patrimonial.

Este delito ha estado tradicionalmente regulado en el Código Penal, pero ha ido sufriendo una serie de modificaciones en las reformas de 2003 y 2010 orientando sus tipos hacia el fenómeno de la ciberdelincuencia. Ya en el propio art.248 se contempla junto con la forma típica de comisión (art.248.1) otra vinculada a los artificios técnicos, siendo esta última la que se ha ido completando en los últimos años, (art.248.2).

Se regula dentro del Título XIII del Libro II del Código Penal, en los art.248 y ss. En ellos se incrimina la acción de quien como consecuencia de una conducta engañosa produce un perjuicio patrimonial en un tercero a favor del disponente.

En el delito de estafa el elemento más relevante es el **engaño,** que constituye el específico desvalor de acción. Forma el elemento que tiene que producirse en un tercero para inducirle a error generando un perjuicio patrimonial en la víctima o en un tercero.

> Este elemento planteó serias dudas con anterioridad a la creación del art.248.2 del Código Penal en los casos de estafas informáticas en las que el autor se sirve de dispositivos electrónicos para llevar a cabo la acción, pues en ellas se consideraba que el elemento del engaño no concurría al ser imposible engañar a una máquina ya que para ello se necesita de un raciocinio, es decir tener voluntad, de lo que las máquinas carecen. De ahí que se entendiera que solo se podía engañar a una persona física y que la estafa se tenía que desarrollar en el marco de una relación *intuitu personae*.

> Todo ello implicaba que el fraude informático era atípico al no darse el elemento del engaño, lo que motivó la inclusión del art.248.2[49].
>
> El concepto ha ido evolucionando, y en la actualidad se ha llegado a proponer que se vea en el contexto de la sociedad contemporánea entendiéndose integrado en los supuestos en que median aparatos automáticos, pues lo relevante es la acción fraudulenta que persigue el error en la víctima y no el dispositivo del que se sirve el autor.

En consecuencia la estafa gira en torno al engaño, sobre el que se han ido construyendo nuevos tipos enfocados a regular nuevas modalidades delictivas, principalmente en el entorno del fraude informático. En este ámbito es precisamente en el que la estafa informática se ha visto más ampliada y regulada en los últimos años, puesto que en ella la conducta se realiza valiéndose de alguna manipulación informática o artificio semejante como indica el art.248.2 CP.

Junto al engaño el delito de estafa presenta una estructura singular, ya que para que se consume se necesita que se cumplan una serie de requisitos de forma causal. Tales requisitos forman en su conjunto los elementos del delito de estafa[50].

> El delito se define en el primer apartado del art.248, en él se regula el tipo básico aunque es aplicable al resto de supuestos de la sección. Es en realidad el tipo que describe la forma clásica por la que se realiza el delito de estafa.
>
> > *"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".*

[49] Vid. MATA Y MARTÍN. R. M., E*stafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago,* Thomson Aranzadi, Navarra, 2007, pp.33-34. El requisito del engaño hacia el tercero, entendido como elemento fundamental del delito de estafa es controvertido en el fraude informático ya que ahí no se está engañando a otra persona sino sirviéndose de artificios técnicos para cometer el delito. Por este motivo se hizo necesario regular específicamente en un apartado distinto la estafa informática, ya que el hecho de actuar sobre una máquina y no sobre una persona dificultaba ver este engaño dentro del tenor literal del art.248.1. Por ejemplo hay supuestos donde se consuma el delito sin la intervención del otro sujeto, con la mera introducción en su ordenador originando una sustracción de activos en su cuenta bancaria. De este modo la acción plantea problemas a la hora de su delimitación penal. Todas estas circunstancias fueron las que hicieron necesaria la aparición de un tipo específico para tales supuestos, ya que como señala la jurisprudencia, "*en los casos en los que el perjuicio se produce directamente por medio del sistema informático, con el que se realizan las operaciones de desplazamiento patrimonial, no se produce ni el engaño ni el error necesarios para el delito de estafa; a las máquinas no se las puede engañar, a los ordenadores tampoco (…), (STS, de 19 de abril de 1991)".* Todo ello hacía que este fenómeno en auge no pudiera ser castigado, pues al faltar el engaño la acción quedaba impune como delito de estafa. También planteaba dudas incluirlo dentro del hurto o en el delito de apropiación indebida. Finalmente con la introducción del segundo número del art.248 el problema quedó solucionado ya que en él se tipifica específicamente el supuesto sin necesidad de ajustarse a los requisitos del tipo básico del art.248.1.

[50] La estructura coincide con la estafa informática que veremos en el siguiente epígrafe. La diferencia radica en la manipulación informática o en el artificio semejante.

Para que la conducta se consume se requiere que se realicen una serie de actos de forma consecutiva, debiendo haber una relación de causalidad entre ellos[51].

En primer lugar es necesaria la acción, una conducta engañosa por la que se induce a error a la otra persona mediante actos externos. El engaño penal es distinto del que se recoge en el ámbito civil con carácter general en el art.1269 CC, ya que en el Derecho penal es necesario realizar un engaño de una gravedad mayor, debe ser determinante para producir el error en la otra persona.

Por tanto el tipo se produce mediante una acción y no una omisión, (salvo ciertos supuestos donde se omite deliberadamente cierta información que de ser expresada impediría la sucesión de hechos[52]).

Al engaño le debe seguir el error que se produce en la otra persona. Es necesario que el engaño haya sido suficiente y que en abstracto sea posible la inducción al error. Además entre ambos elementos debe mediar una relación de causalidad.

Tras el error el sujeto estafado deberá realizar un acto de disposición patrimonial a favor del sujeto activo mediante la entrega de una cosa o la prestación de un servicio. Deben coincidir ambas posiciones en la misma persona, es decir el engañado y el disponente deben ser los mismos.

Finalmente la disposición patrimonial tiene que generar un perjuicio en el patrimonio de la víctima (el engañado) o en el de un tercero. El perjuicio patrimonial al que se vincula el patrimonio es entendido en sentido objetivo y no en abstracto, es decir no se concibe como la posibilidad de haber obtenido un beneficio, sino como una disminución efectiva del mismo a consecuencia de la estafa.

Además durante todo el proceso anterior el autor debe actuar con ánimo de lucro ya que estamos ante un delito de enriquecimiento. También junto al ánimo de lucro se requiere el dolo de generar el engaño en la victima que también debe estar presente en todos los elementos del tipo. En este sentido cabe señalar que no se prevé la comisión culposa del delito de estafa.

Para concluir, se viene entendiendo que el delito se consuma cuando se produce el perjuicio patrimonial sin que sea necesario que el autor se haya aprovechado del mismo, sin embargo la cuestión no es pacífica en la doctrina[53]. En los casos donde no se ha llegado a

[51] MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, pp. 431-436.

[52] Véase la STS, de 6 de diciembre 1974.

[53] Dicha opinión es seguida por parte de la doctrina como MUÑOZ CONDE, sin embargo la cuestión no es pacífica del todo pues otros autores (*Vid.* MATA Y MARTÍN. R. M., E*stafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago,* Thomson Aranzadi, Navarra, 2007, p.104) consideran que para que se consume el delito es necesario que el autor se haya enriquecido, no bastando con que la víctima haya realizado el acto de disposición patrimonial. En este sentido se argumenta que el delito de estafa es un delito patrimonial que busca causar un menoscabo en el patrimonio de la víctima, por ello la disposición

producir el acto de disposición patrimonial pero sí ha habido engaño suficiente por parte del autor, el delito se entendería realizado en grado de tentativa.

1.2 Formas de comisión del fraude informático

Las formas de comisión mediante las que se realiza la estafa informática son de lo más variado pues revisten una serie de comportamientos externos tendentes a obtener un acto de disposición patrimonial. No obstante en su relación interna todas ellas comparten los elementos comunes de este delito que antes se han mencionado, pues constituyen por igual un delito de estafa sin perjuicio de cómo sea llevado a cabo.

En este sentido la propia esencia del delito de estafa permite al autor llevarlo a cabo de múltiples maneras, pues al requerir que sea realizado mediante engaño el autor se puede valer de múltiples elementos fácticos, tanto del mundo virtual como del físico para que le sea más fácil inducir a error a la víctima y producir el acto de disposición patrimonial.

De este modo las conductas por las que se lleva a cabo el delito son susceptibles de ir evolucionando con el paso del tiempo a medida que la tecnología se desarrolla.

En resumen se puede hablar de cuatro técnicas[54]:

A. Obtención de los datos o claves de acceso a determinados servicios y uso indebido de los mismos. *Spyware, phishing y pharming*

Dentro de esta conducta encontramos dos de las técnicas más conocidas en el seno del fraude informático, el ***spyware*** y el ***phishing***.

La primera la forman las conductas mediante las cuales se sustraen datos que permiten la suplantación de personalidad de la víctima. De este modo se obtiene por ejemplo la clave bancaria de un sujeto y se accede a su cuenta como si el autor fuera él.

El modo de llevarla a cabo es mediante archivos espía (*spyware*) que una vez instalados en el ordenador envían información al autor acerca del sistema o de claves de acceso.

---

patrimonial que ella realice debe tener un reflejo en la realidad, incrementando el patrimonio del autor. De este modo si el patrimonio del autor no se incrementa y solo hubiera habido un acto de disposición, el delito no se entiende consumado, siendo punible simplemente en grado de tentativa.

[54] FERNÁNDEZ TERUELO, J., G., *Cibercrimen, los delitos cometidos a través de Internet*, Constitutio Criminalis Carolina, 2007, pp.28-33.

Por su parte, el *phishing* también es otra conducta por la que el autor obtiene claves de la víctima, pero en este caso es ella misma quien se las facilita mediante fórmulas que derivan del propio *phishing*. Lo forman acciones en las que se envían correos electrónicos a la víctima con links hacia páginas simuladas pero con apariencia normal, casi idéntica a la original. En ella requieren a la víctima a que introduzca sus contraseñas o números de tarjetas de crédito, de tal modo que el autor de la estafa las recibe directamente como si se tratara del propietario de la página original.

> De forma similar en este ámbito se incluye el ***pharming*,** mediante el cual el autor modifica las direcciones web para conducir a la víctima mediante las páginas que quiere ver pero que en realidad son otras, en las que proporciona su información personal que llega directamente al autor.

B. *Diarlers*, (conexiones telefónicas fraudulentas)

Los *diarlers* son programas de marcado telefónico que hacen que los dispositivos telefónicos realicen llamadas automáticamente sin autorización de su titular a números de tarifación adicional, es decir de un alto coste para el usuario.

Se producen como consecuencia de la instalación de un programa en el dispositivo sin que el usuario lo sepa. Sin embargo otras veces se instalan junto a otros programas que descarga voluntariamente el usuario, lo que será ilegal siempre que no vengan claramente establecidas en la descripción del programa las consecuencias que acarrea su instalación, es decir la descarga de estos otros programas.

C. Fraudes en operaciones de comercio electrónico

Son fraudes que se producen como consecuencia de actividades de comercio que realizan particulares o empresarios. Suelen dar lugar a supuestos en que la víctima paga el objeto pero nunca llega a recibirlo o lo hace con otras características distintas a las que figuraban en la oferta.

D. Envío de mails fraudulentos

Se trata del envío masivo de correos electrónicos en los que se da la posibilidad a la victima de ganar dinero de un modo aparentemente sencillo, pero para ello previamente hay que realizar un depósito de una cantidad de dinero con la que se pagarán los gastos de tramitación.

Como consecuencia de dicha acción se realizará un cargo en la tarjeta de crédito de la víctima por una compra que nunca sucederá. Además las reclamaciones que tenga serán atendidas en un número de teléfono internacional que se le proporciona, lo que le ocasionará aun más gastos y prolongará la estafa.

2. Bien jurídico protegido

En el delito de estafa informática al igual que en la estafa genérica lo que se protege es el patrimonio ajeno de forma global.

Si bien hay parte de la doctrina que apunta a la protección de la buena fe o de las relaciones fiduciarias[55]. No obstante la regulación está orientada exclusivamente a la protección del patrimonio y en el momento en que resulta menoscabado se produce el delito.

3. Regulación penal. El problema del robo con fuerza en las cosas

3.1 Fraude informático. La manipulación informática

El supuesto concreto de estafa informática aparece regulado en el art.248.2 del Código Penal[56] en tres apartados que fueron incluidos sucesivamente en las reformas de 2003 y 2010.

El tipo básico de la estafa informática le encontramos en el art.248.2.a) que establece:

> *"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".*

Se trata del fraude informático, que reproduce el mismo esquema anterior para las estafas normales pero sin que sea necesario el engaño en sentido estricto al ser sustituido por la **manipulación informática**[57]. De esta forma el tipo es plenamente aplicable a la estafa aunque no requiera el engaño, es decir lo que en la estafa tradicional es el engaño, en

[55] Véase MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, p. 428.

[56] http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t13.html

[57] No obstante sí que cabe apreciar diferencias entre la estafa normal y la informática a pesar de estar ambas tipificadas. En general el fraude informático se ve como una figura afín que se incluye en el concepto, pues como indica MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, pp. 45-56; el artículo no habla de que los autores sean reos de estafa, sino que *se considera* legalmente como tal. Es decir que la regulación trata de asimilarlos pero al indicar ese matiz parece dar a entender que las figuras no son exactamente las mismas y por ello no resulta plenamente aplicable el esquema teórico del tipo básico del delito de estafa. Sin embargo para todo lo demás y las consecuencias que de ello derivan sí que se consideran afines.

la estafa informática es la manipulación informática o el artificio semejante que deberá producir una transferencia no consentida de un activo patrimonial en beneficio del autor y en detrimento del tercero.

La manipulación informática consiste en la alteración por parte del sujeto activo de un sistema informático, tanto la parte física como el software, de tal modo que modifica su correcto funcionamiento, alterando el resultado al que habría de conducir el normal procesamiento automatizado de datos [58].

Es por ello el elemento que más caracteriza esta modalidad de estafa (diferente de la convencional) y con el que se logra la transferencia patrimonial no consentida. De este modo la manipulación informática se configura en nuestra legislación como un elemento indefinido y amplio sobre el que se centra la conducta punible, pues su ambigüedad da pie a una interpretación extensiva.

Dicha manipulación puede producirse de cualquier forma o en cualquier momento del procesamiento o tratamiento automatizado de datos (siempre que sea previa a la disposición patrimonial por parte de la víctima), e incluso desde cualquier lugar[59]. En general se realiza a lo largo de todo el proceso de funcionamiento del sistema informático y del procesamiento de datos que media entre que se han introducido y hasta que salen.

En este sentido caben manipulaciones previas, cuando el autor actúa en los datos sobre los que opera el programa y en la introducción de otros nuevos en el sistema antes de que se haya producido la disposición patrimonial.

La manipulación se puede hacer de forma activa u omisiva: activa modificando datos reales o añadiendo otros ficticios; y omisiva dejando de incorporar al procesamiento de datos los que correspondían, evitando que tal proceso se lleve a cabo correctamente. Esto lo podíamos ver en las conductas fraudulentas que se señalaban al inicio de la sección, donde se podía observar como en ellas se producía dicha manipulación, mandando mensajes de correo falsos o introduciendo archivos en el ordenador que rastreaban las contraseñas por ejemplo. Todas ellas contienen en algún momento de su realización una manipulación informática de los elementos característicos que las forman.

---

[58] CHOCLÁN MONTALVO, J. A., "Infracciones patrimoniales en los procesos de transferencia de datos", en: *El cibercrimen, nuevos retos jurídico penales, nuevas respuestas político criminales, Comares,* Granada, 2006, pp. 75-77.

[59] MATA Y MARTÍN. R. M., E*stafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago,* Thomson Aranzadi, Navarra, 2007, p.71.

La manipulación informática se ve completada por la cláusula abierta de ***"cualquier otro artificio semejante"***[60], lo que permite que el tipo se adelante a la criminalidad y no quede vacío de contenido ante nuevos fenómenos que puedan surgir[61].

Se trata de una modalidad de comisión alternativa de la estafa informática que no requiere la manipulación informática para su consumación, sino la utilización de cualquier otro artificio semejante a ella. De este modo la acción no solo se realiza mediante la conducta genérica de manipulación informática, sino además a través de cualquier otro artificio semejante, lo que permite evitar problemas de aplicación en los casos en que no se pueda hablar en sentido estricto de manipulación informática y así adaptar el precepto a nuevas situaciones que se originen con el rápido desarrollo de las nuevas tecnologías sin tener que modificarle.

En este sentido la citada cláusula resulta útil en los casos de manipulaciones de máquinas automáticas expendedoras de productos o mercancías donde no se aprecia con claridad el aspecto informático de la manipulación. En estos casos se acude al inciso relativo a los artificios semejantes para integrar la situación en el precepto y no vulnerar el principio de legalidad.

Sin embargo ambas modalidades parecen compatibilizarse al calificarse como informático tanto la manipulación como el artificio, debiendo ser vistas de forma conjunta. De este modo se viene entendiendo que la manipulación informática es la cláusula general del precepto y que incluye otras modalidades de comisión (los artificios semejantes) para los casos en que la conducta no se integre estrictamente en el significado de manipulación informática[62].

Por otro lado, la acción por la que se lleva a cabo la transferencia no consentida de un activo patrimonial se puede producir de manera externa, por personas ajenas al sistema que utilizan las diferentes redes que tienen a su alcance; o interna, por miembros que están autorizados a introducirse en él. Incluso cabría llevarla a cabo mediante la actuación conjunta de ambos sujetos.

---

[60] Con esta cláusula se permite abarcar los supuestos en los que no ha habido manipulaciones informáticas que dan lugar al beneficio patrimonial. Además así se colman lagunas en casos donde en lugar de haber una manipulación informática la hay de carácter mecánico. Esto viene siendo cada vez más frecuente donde lo que se manipula son aparatos automáticos como una máquina de tabaco o una recreativa.

[61] MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, pp. 50-51.

[62] MATA Y MARTÍN. R. M., E*stafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago,* Thomson Aranzadi, Navarra, 2007, p.95.

De esta forma es posible realizar el delito por varias personas, lo que nos conduce a las reglas generales de participación delictiva, ya sea en forma de cómplices o de cooperadores necesarios. Estas personas que complementan la acción deben intervenir antes de que se produzca la transferencia de activos patrimoniales. Y cuando dicha acción venga realizada exclusivamente por terceros ajenos al sistema deberá reunir también los mismos requisitos que en el caso general, es decir que se altere el normal desarrollo y resultado del procesamiento automatizado de datos[63].

El resultado del delito debe ser la transferencia patrimonial no consentida, aunque también es posible que sea una prestación de servicios.

Finalmente cabe señalar que junto a la forma activa también puede consumarse de forma omisiva (aunque ello no es lo más habitual ya que el tipo está pensado para que sea realizado de forma activa). Un ejemplo sería el supuesto en que se deja de incorporar al procesamiento de datos los que correspondían, evitando que el proceso se lleve a cabo correctamente.

3.2 Actos preparatorios del delito de estafa

Al supuesto básico del fraude informático se añade desde 2003 (aunque reenumerado en 2010) una nueva conducta en el art.248.2.b) que incrimina a quienes estén en contacto con programas informáticos destinados específicamente a realizar estas actividades fraudulentas.

> *"Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo".*

El precepto contiene una serie de actos preparatorios que facilitan la posterior realización de la estafa y que deben ir dirigidos a su comisión. Entre ellos aparece la fabricación, introducción, posesión o facilitación de programas que permitan llevar a cabo el delito de estafa informática.

El problema que plantea el supuesto es que la conducta es considerada en sí misma como constitutiva de un delito de estafa, estando equiparada al tipo básico previsto en la letra anterior, e incluso siendo castigada con la misma pena. De este modo quien cometa el

[63] MATA Y MARTÍN. R. M., E*stafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago,* Thomson Aranzadi, Navarra, 2007, p.90.

supuesto de la letra b) es igualmente considerado como reo de estafa a pesar de tratarse en realidad de actos preparatorios de ella o incluso de meras tentativas.

Por esta razón el precepto es criticado, y la explicación que desde la doctrina[64] se viene dando a dicha equiparación penal reside en la importancia que tienen para el tráfico económico tales conductas, pues con ellas se vulnera el sistema informático en su conjunto, entendido como un bien jurídico colectivo susceptible de ocasionar un perjuicio patrimonial a la sociedad.

De este modo la reforma es fruto del perjuicio que generan las estafas en el tráfico económico y refleja el incremento de la delincuencia informática en este ámbito en los últimos años, propiciado en parte por el auge de los nuevos dispositivos electrónicos que facilitan su comisión.

Por ello la conducta se configura como un delito de peligro abstracto, y que de consumarse lo hará junto a la de la letra anterior, el tipo básico, produciéndose un concurso de delitos entre ambos.

Finalmente para que el delito se consume es necesario que quien realice tales actos lo haga con la intención de cometer posteriormente el delito de estafa, pues el precepto incluye ese especial tipo subjetivo que debe concurrir en todo momento en la realización de la acción. De este modo solo se contempla la comisión dolosa, y nunca la culposa.

3.3 El uso de tarjetas de crédito por personas ajenas al titular. El problema del robo con fuerza en las cosas

La regulación de la estafa informática se completa con el art.248.2.c), que fue introducido con la reforma de 2010 para solventar los problemas que generaba el uso de tarjetas de crédito y demás instrumentos financieros por personas ajenas a su titular. En este punto la doctrina no estaba de acuerdo en cómo calificarlo, pues para algunos podía tratarse de un delito de robo con fuerza en las cosas, mientras que para otros se incluía dentro del fraude informático[65] [66].

[64] MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, p. 430.
[65] Véase MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, p.434.
[66] Véase más ampliamente CHOCLÁN MONTALVO, J. A., "Infracciones patrimoniales en los procesos de transferencia de datos", en: *El cibercrimen, nuevos retos jurídico penales, nuevas respuestas político criminales, Comares,* Granada, 2006, pp. 80-89.

Con anterioridad a dicha reforma el uso de tarjetas de crédito de terceros, la utilización abusiva del cajero por su titular o el uso de tarjetas de crédito falsas daban problemas de delimitación jurídico penal al no poderlas encajar en ninguna figura delictiva.

- Respecto al uso de tarjetas de crédito de terceros el problema no radicaba en el hecho de sustraer la tarjeta al legítimo titular (que vendría encuadrado en la figura delictiva del robo, hurto, apropiación indebida…), sino en su posterior uso en el cajero. Es una acción distinta que no puede ser considerada como estafa al no concurrir el requisito del engaño y llevarse a cabo en un momento temporal y especial diferente a la sustracción, incluso con un sujeto activo distinto.

  De este modo la naturaleza jurídico penal que se otorgue al engaño permitirá subsumirlo en una figura jurídica distinta, lo que dará lugar a consecuencias distintas dependiendo de la que sea.

  En este sentido para considerar a la acción como un delito de estafa se requieren actos personales, directos e inmediatos de engaño a otra persona física. Sin embargo tales requisitos no se producen en el caso de la utilización de tarjetas de crédito de terceros al no haber contacto directo entre autor y víctima. Por ello en primer lugar se descarta la posibilidad de aplicar la versión clásica del delito de estafa[67].

  Por este motivo en España la jurisprudencia vino reconduciendo en un primer momento la acción al delito tradicional de estafa del art.248.1 CP, pero como consecuencia de la falta de aplicación del engaño, (al ser imposible su eficacia sobre máquinas), y la concepción personal de la estafa, (que requiere un contacto directo de carácter físico entre dos personas, *intuitu personae*, no de persona y máquina), se vio que dicha solución que no era la correcta.

  De este modo se concluyó que la utilización fraudulenta de las tarjetas de crédito para producir un perjuicio patrimonial en la víctima o en un tercero no puede encajarse en ese artículo, por lo que no se soluciona el problema de su naturaleza al no quedar reconducida ni en el delito de robo ni en el de estafa.

[67] MATA Y MARTÍN, R. M., "Infracciones penales con tarjetas de pago", en: *Separata de Infraçoes Económicas e Financeiras*, Estudos de Criminologia e Direito, Coimbra Editora, pp.601-602

Por tanto la solución pasó por aplicar tales supuestos en la conducta descrita en el art.248.2.a), integrando la acción de la persona que la realiza en la expresión de *artificio semejante* a la que alude el precepto cuando establece *"quienes consigan una transferencia patrimonial no consentida habiendo utilizado manipulaciones informáticas o artificios semejantes (…)"*.

Era quizá una interpretación demasiado extensiva de ese tipo penal pero una de las pocas soluciones que permitían dar solución a este problema en esa época anterior a la reforma de 2010.

Cuando esta reforma se llevó a cabo el problema se solucionó, pues el nuevo art.248.2.c) contempla expresamente la conducta de *"quienes usando tarjetas de crédito realicen operaciones de cualquier clase en perjuicio de su titular (…)"*. Esta nueva letra acaba definitivamente con los problemas al tratar la situación que venimos describiendo cuando menciona a las tarjetas de crédito, y dando una regulación concreta a las controversias que ocasionaban.

- De forma paralela al uso fraudulento de las tarjetas de crédito por terceros también generó problemas el uso de cajeros automáticos de las entidades financieras cuando se introducían en ellos tarjetas que eran usadas irregularmente para obtener cantidades de dinero en metálico.

  Su encaje jurídico penal pasó por reconducir tales acciones a un supuesto de robo con fuerza en las cosas al considerar como llave a la tarjeta con que se realizan tales acciones. Sin embargo en un primer momento esa equiparación no estaba prevista en el Código Penal, por lo que hubo que interpretar extensivamente la regulación que se daba en el delito de robo con fuerza en las cosas, y dentro de este lo que consideraba por llave en el art.239.

  El problema se solucionó definitivamente tras la reforma de 2010 en la que se introdujo un último inciso en el art.239 según el cual pasaban también a considerarse como llaves "*las tarjetas, magnéticas o perforadas y los mandos o instrumentos de apertura a distancia"*.

  De este modo el supuesto ahora encuentra un encaje pleno en la ley siendo de aplicación a los supuestos en que los autores sirviéndose de tarjetas falsas proceden a retirar dinero de los cajeros.

- Finalmente cabe señalar un último problema, cuando la tarjeta es usada por el titular de la misma pero sin que tenga fondos suficientes o habiendo sobrepasado su periodo de vigencia.

  Para solucionarlo la doctrina y la jurisprudencia apelan a la diligencia que debe tener la víctima para comprobar tales aspectos de la tarjeta, puesto que sin ella la acción del autor no sería considerada como engañosa al no contener el engaño suficiente que debe de inducir a error a la víctima. En este sentido la persona con la que se contrata debe comprobar la validez de la tarjeta y no actuar de manera negligente[68].

  En estos casos se puede llegar a considerar que la acción carece de responsabilidad penal teniendo que acudir exclusivamente a la vía civil para que el autor reintegre la cantidad adeudada. Esto significa que el mero hecho de un pago realizado con una tarjeta propia sin fondos suficientes no debe constituir por sí mismo un hecho típico que genere responsabilidad penal, pues a esa conducta habrá que añadir todos los elementos genéricos del delito de estafa antes señalados, así como el dolo de perjudicar a la víctima.

Por todo lo anterior vemos como el principal problema relativo al uso de tarjetas de crédito de terceros queda solucionado en 2010 mediante la reforma del Código Penal que introdujo la Ley Orgánica 5/2010, al añadir una tercera letra al art.248.2, la 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".*

Se trata de ampliar el supuesto de los fraudes informáticos a esta nueva realidad. El nuevo tipo se aleja de la figura tradicional de las estafas y tipifica un supuesto concreto que en algún elemento como el del engaño queda desdibujado.

[68] MATA Y MARTÍN. R. M., E*stafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago,* Thomson Aranzadi, Navarra, 2007, pp. 39-40.

Para concluir la Sección cabe señalar que en la reforma del Código Penal introducida por la LO 1/2015 no se incluyen modificaciones relevantes en el fraude informático, aunque si lo hacen otros preceptos a nivel general para la estafa tradicional[69].

[69] Se prevé una modificación del art.249 en relación a las penas y se da una nueva redacción al art.250 sobre los agravantes al incluir un supuesto cualificado cuando el valor de lo defraudado supere los 250.000 euros. En la anterior redacción el límite se fijaba en 50.000 euros, siendo el agravante normal.

SECCIÓN CUARTA: **DELITOS CONTRA LA PROPIEDAD INTELECTUAL**

1. Introducción. Programas de ordenador y bases de datos

Como venimos señalando, la actual sociedad de la información está en continuo desarrollo debido al incremento de las nuevas tecnologías y artificios semejantes. Todos ellos permiten un aumento de la productividad y eficiencia en todos los campos, desde el empresarial hasta el institucional o incluso el familiar.

La contribución a este desarrollo ha venido propiciada principalmente por los elementos que participan en el tráfico jurídico empresarial y que permiten la reproducción, almacenamiento y transmisión de sus componentes. De esta forma una parte importante del tráfico jurídico y económico actual es la propiedad intelectual, que se define según el art.2 del Texto Refundido de la Ley de Propiedad Intelectual (TRLPI) como *todos los derechos de carácter personal y patrimonial, que atribuyen al autor la plena disposición y el derecho exclusivo a la explotación de la obra, sin más limitaciones que las establecidas en la Ley*[70].

El contenido de la propiedad intelectual lo forman las obras de carácter literario, artístico o científico. Este contenido se interpreta de un modo bastante amplio, pues se compone de todas las obras que el art.10 incluye, tales como libros, informes, conferencias, composiciones musicales, obras de teatro o dramáticas, esculturas, proyectos, gráficos, obras fotográficas, programas de ordenador e incluso las bases de datos del art.12.

De todo el elenco de obras cabe destacar a los **programas de ordenador y bases de datos**, pues constituyen el objeto material protegido por el Derecho penal en el ámbito de la ciberdelincuencia en materia de propiedad intelectual.

Los programas de ordenador como parte del contenido de la propiedad intelectual forman parte de la sociedad de la información y de las nuevas tecnologías contribuyendo a su pleno desarrollo. Sirven de fundamento a gran parte del desarrollo tecnológico, social y

[70] http://noticias.juridicas.com/base_datos/Admin/rdleg1-1996.l1t1.html#l1

económico al que se está viendo sometida la sociedad en su conjunto al constituir el motor de crecimiento a través del cual se apoya gran parte del tráfico jurídico, pues facilita enormemente su actividad incrementando la productividad y eficiencia. De ahí que deban ser objeto específico de protección.

El auge e importancia que están experimentando en la actualidad queda patente en todos los ámbitos, ya sean públicos, privados o familiares. En este sentido no debemos olvidar que por programa de ordenador el art.96 TRLPI entiende a *toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.*

Como vemos el concepto es amplísimo, puesto que sustenta todo software del que se compone un sistema informático para que este realice sus tareas. Por ello no debemos circunscribir sus funciones a un mero ámbito residual para quien trabaja con ellos ya que el concepto está dentro de todo software capaz de realizar las actividades descritas. Son el sustento de todas las nuevas tecnologías, por lo que se hace necesario ser conscientes de su utilidad y de que constituyen el motor del progreso económico y social.

> Como consecuencia de lo anterior ha sido necesario incrementar su protección en una triple dimensión, ya que han aumentado las conductas delictivas que vulneran los ordenadores y las bases de datos:
>
> - Por un lado mediante los programas destinados a su inutilización, los virus, en cualquiera de sus modalidades. Se encuentran tipificados en el art.264 dentro del delito de daños.
>
> - Además estas conductas se pueden castigar desde el punto de vista de los robos o hurtos cuando el autor se apodera de ellos de una forma física.
>
> - Y finalmente mediante la piratería, es decir la actividad delictiva que tiende a comercializar copias no autorizadas de los programas informáticos. Su ámbito delictivo engloba el plagio, la reproducción, la comunicación y la distribución de las obras objeto de protección.
>
> En esta tercera dimensión es donde el Derecho penal encuentra su ámbito de aplicación en relación a los delitos informáticos contra la propiedad intelectual, pues comprende las conductas ilícitas de quienes se aprovechan del ingenio ajeno para lucrarse. Además tales conductas desincentivan la creación de nuevos

> programas y de obras en general ya que los autores son conscientes de las pocas garantías que existen de protección hacia sus obras. Todo ello provoca que se deje de invertir en este tipo de obras impidiendo el progreso.

Su importancia es tal para la sociedad que es necesario tutelar jurídicamente la propiedad intelectual para garantizar la protección de las obras literarias, artísticas y científicas en general y de los programas informáticos en particular.

Para ello desde el punto de vista mercantil se ha reformado el Texto Refundido de la Ley de Propiedad Intelectual mediante la ley 21/2014, de 4 de noviembre, que ha entrado en vigor el pasado enero de 2015[71] y que sirve de apoyo al resto de legislaciones al contener los caracteres básicos que delimitan su contenido y aplicación. Además es útil a la hora de entender los conceptos que usa la regulación penal cuando habla de plagio, comunicación, distribución o reproducción.

Junto a esa ley ha sido preciso incorporar nuevos tipos penales específicos que sancionen de forma más contundente las conductas más graves en esta disciplina, por lo que el Código Penal cuenta desde 1995 con los art.270-272 dentro de la Sección primera del Capitulo XI del Título XIII relativo a los delitos contra el patrimonio y el orden socioeconómico.

Los comportamientos que se castigan en tales artículos afectan al desarrollo tecnológico de la sociedad, impiden su avance y constituyen una fuente de pérdidas económicas enorme para sus creadores. En este sentido destaca un informe realizado por el Observatorio Mundial contra la Piratería de la UNESCO[72] el pasado 2013 que indica que el mercado de la piratería mueve unos 16.000 millones de euros.

2. Bien jurídico protegido

Del art.2 TRLPI se extrae que el bien jurídico es la propiedad intelectual en su vertiente patrimonial. Además del propio Código Penal se deduce la misma conclusión al estar regulado en el título XIII dedicado al patrimonio y el orden socioeconómico.

No obstante la concepción penal de la propiedad intelectual es diferente del ámbito civil, y así lo hace saber el legislador al distinguir ambas mediante la exigencia del dolo en la

[71] http://www.boe.es/boe/dias/2014/11/05/pdfs/BOE-A-2014-11404.pdf
[72]http://www.unesco.org/new/es/culture/themes/creativity/creative-industries/world-anti-piracy-observatory/

vertiente penal, que no contempla en ningún caso la comisión culposa, cumpliendo de este modo con el principio de intervención mínima del Derecho penal.

De ahí que aunque para entender los elementos del tipo penal haya que acudir a la legislación civil, esta es accesoria ya que el ámbito penal tiene virtualidad por sí mismo. Lo mismo sucede con la concepción del bien jurídico propiedad intelectual, que difiere de la que tiene el Derecho privado.

De este modo la protección de los art.270 y siguientes en materia de propiedad intelectual se centra como dice MIRO LLINARES[73] en los "*intereses patrimoniales de los titulares de derechos de explotación exclusiva de propiedad intelectual, no tutelando en la vía penal ni los intereses morales del autor*". Por tanto para este autor la protección que otorga el Derecho penal es estrictamente patrimonial, y las vulneraciones que atenten contra otros bienes jurídicos quedarán excluidas de la tutela penal.

Frente a esa corriente patrimonialista, otros autores como MUÑOZ CONDE[74] consideran que también hay una protección penal extra patrimonial de carácter moral frente a acciones como el daño moral. Para este autor junto con la protección eminentemente patrimonial que reconoce el art.270, se encuentran otras como las que castigan el plagio, en las que al proteger el derecho del autor a la paternidad de su obra lo que se hace es proteger un contenido superior al patrimonial.

Por tanto lo que es indudable es que en esta Sección relativa a la propiedad intelectual lo que se protege es su contenido patrimonial, sin perjuicio de ciertos comportamientos que en algún caso concreto pueden ir más allá del aspecto puramente patrimonial. Sin embargo para que ellos sean punibles se requerirá que junto al daño moral o extrapatrimonial concurra otro de carácter patrimonial que permita cuantificarlo, ello será lo que motive la intervención del Derecho penal.

3. Regulación penal. Los tipos básico y atenuado de los delitos contra la propiedad intelectual

Como se ha venido señalando en los anteriores epígrafes, el Código Penal ha tipificado una serie de conductas tendentes a proteger todos los derechos de autor que se reconocen a los creadores de las obras.

---

[73] MIRÓ LLINARES, F., *Internet y delitos contra la propiedad intelectual*, Datautor, Madrid, 2005, p. 140.
[74] Véase MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, p. 492.

Dicha protección se regula entre los art.270-272, en el Capitulo XI del Título XIII, que han sido recientemente modificados por la reforma del Código Penal que ha introducido la LO 1/2015.

Esta reforma en materia de propiedad intelectual y a diferencia de lo que ha hecho en otros delitos como el de daños o contra la intimidad, no ha introducido nuevos artículos sino que ha dado una nueva redacción a los ya existentes añadiendo en ellos ciertos matices que amplían las conductas punibles y alteran las conductas tradicionales de los mismos. Además ha organizado mejor la estructura de la sección y ha añadido nuevos números al art.270 como veremos a continuación.

3.1 El tipo básico y las conductas de plagio, reproducción, comunicación y distribución. Especial referencia al tipo subjetivo

Su regulación comienza en el art.270[75], en cuyo primer número se establece el tipo básico de los delitos contra la propiedad intelectual. Las conductas que se castigan frente a la piratería son la reproducción, el plagio, la distribución, y la comunicación pública de la obra.

> *"Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios".*

En primer lugar es necesario realizar unas consideraciones previas de este artículo antes de entrar a analizar las conductas punibles.

Los comportamientos que en él se señalan han ser puestos en relación a los programas informáticos y bases de datos electrónicas de creación intelectual[76] que deben estar en un soporte en el que se puedan plasmar. No pueden ser meras ideas, aunque este soporte puede ser cualquiera como dice el art.10 TRLPI y el propio art.270 CP, que tras la reforma ha incluido un inciso al final por el que se permite que la obra esté en cualquier tipo de soporte o medio.

---

[75] http://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3439.pdf

[76] MATA Y MARTÍN R. M., "Perspectivas sobre la protección penal del software", en: *El cibercrimen, nuevo retos jurídico-penales, nuevas respuestas político criminales*, Comares, Granada, 2006, pp 103-104.

Además los programas han de ser originales según criterios de temporalidad, singularidad o en función de sus novedosos resultados. En definitiva, que el programa no sea una copia de otro, lo que implica que si un programa varía respecto de otro también gozaría de la protección del art.96.3 TRLPI y por ende del Derecho penal.

La conducta que el artículo describe forma el tipo básico en materia de propiedad intelectual, y entra en relación con los delitos informáticos cuando el objeto material sea un programa de ordenador o una base de datos informáticos.

El sujeto activo puede serlo cualquiera, puesto que se trata de un delito común en el que el Código no exige ningún requisito para su realización.

En cambio el sujeto pasivo[77] debe ser alguien que tenga derechos de autor, es decir que pueda explotar la obra (ya sea el propio autor o las personas a las que se lo haya cedido[78]). Por tanto entre tales sujetos encontramos al autor de la obra, (titular original de sus derechos); al transformador; al cesionario, tanto inter-vivos como mortis-causa, siempre que realice esa tarea de forma exclusiva; y a los titulares de derechos conexos, como por ejemplo el intérprete o el traductor.

El objeto material del delito tiene que ser una obra de carácter literario, artístico o científico sobre la que recaigan las conductas punibles de reproducción, plagio, distribución o comunicación. Además esas mismas conductas pueden incidir en la transformación, interpretación o ejecución artística de tales obras, siendo indiferente que estén fijadas en cualquier tipo de soporte o comunicadas a través de cualquier medio.

Para completar lo que se entienden por obras artísticas, científicas o literarias se debe acudir a la legislación mercantil, pues en los art.10-13 TRLPI aparece lo que se entiende por ello[79] y lo que excluye[80].

---

[77] MIRÓ LLINARES, F., *Internet y delitos contra la propiedad intelectual*, Datautor, Madrid, 2005, p. 149.

[78] El TRLPI en sus art.5-9 regula la cuestión de la autoría al establecer quiénes pueden considerarse como tales. Entre sus disposiciones establece que la autoría pertenece a quien ha creado la obra, incluso se presume como tal a la persona cuyo nombre o firma figura en ella.

[79] La ley parte de realizar una enumeración de todas las obras en función de si son literarias, artísticas o científicas. Entre ellas engloba los libros, folletos, impresos, epistolarios, escritos, discursos y alocuciones, conferencias, informes forenses, explicaciones de cátedra; las composiciones musicales; las obras dramáticas y dramático-musicales, las coreografías, las pantomimas y, en general, las obras teatrales; las obras cinematográficas y cualesquiera otras obras audiovisuales; las esculturas y las obras de pintura, dibujo, grabado, litografía y las historietas gráficas, tebeos o cómics, así como sus ensayos o bocetos; los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería; los gráficos, mapas y diseños relativos a la

De este modo el art.270 se remite al TRLPI debiendo acudir a sus disposiciones para entender el concepto de cada uno de los elementos que forman el objeto material. Sin embargo el hecho de tener que acudir a esa otra disposición genera una gran inseguridad, puesto que la enumeración que hace de las obras protegidas es bastante ambigua, sin una descripción acorde de muchas de ellas y sin entrar en su contenido.

En cualquier caso, para concretar el objeto material resulta imprescindible acudir a tales disposiciones del TRLPI.

En los artículos 14 y siguientes aparecen las acciones que están castigadas penalmente, es decir las conductas típicas del art.270, (reproducción, plagio, distribución, y comunicación pública).

Para su comprensión resultan de nuevo útiles las definiciones que proporciona el TRLPI. No obstante el Texto es algo auxiliar pues las conductas penales son independientes de la legislación mercantil aunque compartan el mismo nombre, ya que no se trata de un desarrollo de las mismas. De este modo no se trata de definiciones que automáticamente integran el contenido del art.270.

Tales conductas se pueden diferenciar en dos categorías[81], las que afectan al derecho moral y las que lo hacen a los derechos de explotación. Entre las primeras se encuentra el plagio, regulado entre los art.14-16 TRLPI; y en las segundas la reproducción, distribución, comunicación, exportación e importación, entre los art.17-23 TRLPI.

3.1.1 Plagio

Es una conducta que atenta contra los derechos morales del autor, entre los que se encuentran los derechos sobre su divulgación o el nombre bajo el que se publica[82].

topografía, la geografía y, en general, a la ciencia; las obras fotográficas y las expresadas por procedimiento análogo a la fotografía; los programas de ordenador. A ello añade las traducciones y adaptaciones; las revisiones, actualizaciones y anotaciones; los compendios, resúmenes y extractos; los arreglos musicales y cualquier otra transformación que experimente la obra. Finalmente añade las colecciones de obras ajenas, de datos o de otros elementos independientes como las antologías.

[80] Las disposiciones legales o reglamentarias y sus correspondientes proyectos; las resoluciones de los órganos jurisdiccionales; y los actos, acuerdos, deliberaciones y dictámenes de los organismos públicos.

[81] MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, p. 494.

[82] Entre esos derechos de los que dispone el autor se encuentran los relativos a decidir si su obra ha de ser divulgada y en qué forma; determinar si tal divulgación ha de hacerse con su nombre, bajo seudónimo o signo, o anónimamente; exigir el reconocimiento de su condición de autor de la obra; exigir el respeto a la integridad de la obra e impedir cualquier deformación, modificación, alteración o atentado contra ella que suponga perjuicio a sus legítimos intereses o menoscabo a su reputación; modificar la obra respetando los

Se han dado muchos conceptos para definir la conducta, pero en general se entiende que el plagio constituye una acción por la que el sujeto activo copia una obra ajena en su aspecto sustancial. Tal conducta fraudulenta tiende a usurpar la condición del creador imitando su posición y exteriorizándola por parte del sujeto activo como si fuera suya una obra con características similares a la original[83].

La similitud entre ambas obras (la original y la plagiada) es necesaria para considerar esta acción, debe haber una identidad sustancial para que se esté ante esta figura delictiva. Y además es necesario que la víctima sea el autor legal de la obra.

Del concepto anterior se extrae el elemento central de la conducta que la distingue del resto de acciones que infringen los derechos de propiedad intelectual. Se trata de la negación de la paternidad al autentico creador[84], pues en el resto de conductas típicas se vulneran los derechos de explotación, pero en ninguna se niega la autoría original. No obstante en el plagio no es suficiente con negar la autoría original sino que además hay que atribuirla falsamente a otra persona.

En la realización de la conducta se necesitan dos requisitos, por un lado se requiere una falsa atribución de la autoría de una obra, ya sea en todo o en parte de la misma; y además que la obra se explote ilícitamente mediante conductas tendentes a ello, tales como la reproducción o la comunicación.

De este modo en la conducta se mezclan elementos relacionados con los derechos morales y de explotación del autor. Para la consumación del delito no basta con la vulneración de los primeros (es decir la negación de la paternidad de la obra), sino que además se necesita que haya una vulneración de los derechos de explotación, mediante una conducta de reproducción, distribución o comunicación[85].

Por tanto para que se produzca el desvalor de acción es necesario que haya una lesión efectiva del derecho del autor mediante la distribución de la obra, o incluso abstracta con su reproducción.

Sin embargo como venimos señalando no es plenamente aplicable el concepto civil del TRLPI, pues en el ámbito penal es preciso que se dé el especial tipo subjetivo marcado por el ánimo de obtener un beneficio económico directo o indirecto, lo que en el civil no sucede.

---

derechos adquiridos por terceros y las exigencias de protección de bienes de interés cultural; retirar la obra del comercio, por cambio de sus convicciones intelectuales o morales, previa indemnización de daños y perjuicios a los titulares de derechos de explotación; o acceder al ejemplar único o raro de la obra cuando se halle en poder de otro, a fin de ejercitar el derecho de divulgación o cualquier otro que le corresponda.

[83] MATA Y MARTÍN, R. M., "Perspectivas sobre la protección penal del software", en: *El cibercrimen, nuevo retos jurídico-penales, nuevas respuestas político criminales*, Comares, Granada, 2006, p. 109.

[84] MIRÓ LLINARES, F., *La protección penal de la propiedad intelectual en la sociedad de la información,* Dykinson, Madrid, 2003, p.375.

[85] Del mismo autor, p.379.

3.1.2 Reproducción

Según el art.18 TRLPI es la fijación directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma de toda la obra o de parte de ella, que permita su comunicación o la obtención de copias.

Se trata de una conducta aparentemente alejada de la vulneración de los derechos de propiedad intelectual pero que en realidad en esencial, ya que la realización de copias de la obra o la fijación de las mismas es la base para la posterior realización de otras conductas lesivas de los derechos de propiedad intelectual, como por ejemplo la distribución o la comunicación[86]. Se adelantan de este modo las barreras de protección penal.

Para poder realizar la acción sin incurrir en el tipo penal es preciso estar autorizado. En el caso de los programas de ordenador, según indica el art.99 TRLPI sucede lo mismo incluso cuando la reproducción sea para uso personal. Este requisito exige no sólo la imposibilidad de obtener copias de la obra sin el permiso del autor, sino también el hecho de realizar la fijación de la obra en un soporte duradero sin el permiso del mismo.

Para estar ante esta conducta se requiere que haya una identidad entre la obra original y la que se reproduce, a la vez que tendrá que hacerse de forma repetida, no individualizada. En este sentido cabe limitar la pena en atención a su gravedad como el art.270.4 CP matiza.

Debe tratarse en definitiva de una imitación, que la haga exacta a la original, ya sea en todo o en parte como menciona el art.18 TRLPI. En este sentido, para considerar si se ha producido el ilícito penal cuando se haya reproducido una parte de la obra habrá que atender a criterios cuantitativos y cualitativos que impliquen una cierta entidad o amplitud respecto del total de la misma[87].

Para la consumación de la acción no parece necesario que haya que obtener las copias de forma definitiva, puesto que el propio art.18 TRLPI habla de su *fijación en un soporte* que sea susceptible de generar copias en un futuro, que deberá aportar permanencia o estabilidad a la obra. En el caso de programas de ordenador basta con la mera puesta a disposición del autor en Internet. Además no es preciso que a la reproducción la sigan otras conductas posteriores como la distribución[88].

No obstante en general la concepción sobre el momento en el que se consuma es bastante amplia ya que en el momento en que se obtiene el programa de manera autónoma de la copia se considera consumado. Además el mundo de la informática se caracteriza por la intangibilidad, lo que desdibuja el requisito del soporte.

---

[86] MIRÓ LLINARES, F., *La protección penal de la propiedad intelectual en la sociedad de la información,* Dykinson, Madrid, 2003, p.360.

[87] Del mismo autor, véase p. 363.

[88] MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, p.92.

A juicio del tenor literal del art.270 CP no parece exigirse un mínimo de copias reproducidas por el autor para la realización del tipo. Por tanto resulta irrelevante la cuantía de copias obtenidas mediante dicha conducta, si bien tendrán que vulnerar el bien jurídico, esto es producir una lesión en los derechos de explotación exclusiva del titular. De este modo aunque no se exijan requisitos cuantitativos a la hora de realizar las copias sí que es precisa la lesión del bien jurídico, esto se producirá muchas veces en una ulterior conducta de distribución (la cual en sí misma tampoco se exige para que se consume la reproducción).

Por tanto aunque la conducta de reproducción se regule aisladamente y se pueda consumar con independencia del resto, en la práctica por las exigencias del tipo subjetivo y de la lesión al bien jurídico se hará necesario el concurso con el resto de conductas.

Como se ha ido señalando, todo lo anterior deberá ir acompañado del tipo subjetivo específico relativo al ánimo de obtener un beneficio económico directo o indirecto.

En el entorno de los programas de ordenador y las bases de datos en particular, el ilícito se cometerá mediante un programa que permita la copia, o en su defecto a través de la red con ordenadores conectados entre sí haciendo uso de Internet y de sus diferentes portales, siendo para ello necesario una reproducción masiva, careciendo de responsabilidad cuando la conducta se realice con fines privados.

La responsabilidad se exime en el momento en que el autor presta su consentimiento para llevar a cabo esta actividad. Pero en el caso de la informática, la ley señala en su art.100 TRLPI unos supuestos donde también exime la responsabilidad[89]. Esto sucede en relación al necesario funcionamiento del sistema; por motivos de copias de seguridad; o cuando sea indispensable para obtener la información necesaria para la interoperabilidad de un programa creado de forma independiente con otros programas.

Además de ello, la realización de copias para uso privado tampoco supone la vulneración de los derechos de explotación exclusiva del autor, lo que conduce a la atipicidad de la conducta como indica el art.31 TRLPI.

3.1.3 Distribución

De acuerdo al art.19 TRLPI es la puesta a disposición del público del original o de las copias de la obra en un soporte tangible, mediante su venta, alquiler, préstamo o de cualquier otra forma.

[89] MATA Y MARTÍN, R. M., "Perspectivas sobre la protección penal del software", en: *El cibercrimen, nuevo retos jurídico-penales, nuevas respuestas político criminales*, Comares, Granada, 2006, p. 120.

Se trata de una acción dinámica que no entra en el contenido de la obra sino que se consuma con la puesta en circulación de copias o del original de la obra. Debe haber para ello un ofrecimiento al que le debe seguir la puesta en circulación, ya que de lo contrario sería un acto de preparación e incluso una posible tentativa si ha habido un inicio de ejecución. Es decir que se requiere que la obra sea puesta a disposición del público y que se realicen actos de publicidad sobre ella[90].

No obstante por la mera naturaleza de la acción, previamente a la distribución se producirá una comunicación pública hacia una pluralidad de sujetos, que dará lugar a la efectiva distribución. Esta comunicación puede ser considerada un acto preparatorio, por lo que la mera oferta no constituye la realización del tipo sino que tendrá que dar lugar después a su envío. Y en cualquier caso la distribución será un paso posterior a la reproducción de la obra puesto que así se posibilita al autor la posibilidad de controlar el destino que tendrá la obra una vez haya sido introducida en el comercio[91].

En este sentido para que se consume el delito no basta con el mero ofrecimiento, sino que debe haberse distribuido efectivamente y estar a disposición de los adquirentes, pues de lo contrario el delito se realizaría en grado de tentativa.

A todo ello deberá acompañarle una publicidad hacia una pluralidad de destinatarios, pues se requiere que la distribución quede al alcance de una gran cantidad de sujetos, es decir que haya una extensión cuantitativa[92].

3.1.4 Comunicación pública

El art.20 TRLPI lo entiende como todo acto por el cual una pluralidad de personas puedan tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas. Este supuesto le encontramos por ejemplo en páginas de Internet que permiten el visualizado de una obra sin su previa descarga.

Genera un acceso a la obra para el público en general pero sin que se les distribuya nada. Irrumpe en el mercado poniendo a disposición de una pluralidad de personas la obra artística, científica o literaria lesionando las expectativas de ganancia derivadas de ser el único titular legal autorizado a poner a disposición de terceros tales obras[93].

La conducta se realiza en general por cualquier acto que suponga el acceso no autorizado a la obra sin que haya habido una previa distribución. En este sentido el propio artículo

[90] MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, p.95; y del mismo autor "perspectivas sobre la protección penal del software", en: *El cibercrimen, nuevo retos jurídico-penales, nuevas respuestas político criminales*, Comares, Granada, 2006, pp. 121- 122.

[91] MIRÓ LLINARES, F., *La protección penal de la propiedad intelectual en la sociedad de la información,* Dykinson, Madrid, 2003, p.387.

[92] MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, p.96.

[93] MIRÓ LLINARES, F., *La protección penal de la propiedad intelectual en la sociedad de la información,* Dykinson, Madrid, 2003, pp.399-400.

menciona una serie de conductas consideradas como actos de comunicación pública[94], entre las que destacan las realizadas mediante representaciones escénicas, proyecciones, radiodifusión por vía satélite, por hilo cable, o simples exposiciones.

Las conductas señaladas en el precepto del TRLPI no forman un catálogo cerrado pues cualquier otra forma de comunicación pública supondrá la realización de la conducta punible en el art.270 CP.

En el supuesto de los programas de ordenador se llevará a cabo mediante Internet, y dentro de este se escogerá el modo de realizarlo, pudiendo abarcar más o menos destinatarios lo que afectará a la gravedad del hecho. Depende por tanto del medio elegido que el tipo se realice o no, pues si el medio permite un acceso a una pluralidad de personas dará lugar a la consumación del delito dentro de la modalidad de comunicación pública; y en cambio si las personas a las que les llega la publicidad son insignificantes, no podrá consumarse el delito en cuanto a la infracción de los derechos de autor de un programa informático[95].

Finalmente será preciso que la comunicación se produzca de forma pública y no de forma individual, familiar o doméstica, lo cual excluiría la responsabilidad penal.

3.1.5 Transformación, interpretación o ejecución artística

Según el art.21 TRLPI se entiende por transformación la traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente.

Son conductas en las que sobre la base de la obra original se obtiene otra, pero sí de ello resultaran derechos de autor distintos del primero, el nuevo autor será quien lo podrá transformar, ejecutar o interpretar.

Por tanto son conductas accesorias a la vulneración de los derechos de propiedad intelectual y que carecen de relevancia en el ámbito de la ciberdelincuencia en relación a los programas de ordenador.

---

[94] El art.20 TRLPI incorpora como conductas de comunicación pública, las representaciones escénicas, recitaciones disertaciones y ejecuciones públicas de las obras dramáticas, dramático-musicales, literarias y musicales mediante cualquier medio o procedimiento; la proyección o exhibición pública de las obras cinematográficas y de las demás audiovisuales; la emisión de cualesquiera obras por radiodifusión o por cualquier otro medio que sirva para la difusión inalámbrica de signos, sonidos o imágenes; la radiodifusión o comunicación al público vía satélite de cualesquiera obras; la transmisión de cualesquiera obras al público por hilo, cable, fibra óptica u otro procedimiento análogo; la retransmisión de la obra radiodifundida; la emisión o transmisión, en lugar accesible al público, mediante cualquier instrumento idóneo, de la obra radiodifundida; la exposición pública de obras de arte o sus reproducciones; la puesta a disposición del público de obras, por procedimientos alámbricos o inalámbricos; el acceso público en cualquier forma a las obras incorporadas a una base de datos; La realización de cualquiera de los actos anteriores, respecto a una base de datos.

[95] MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, p.95; y del mismo autor "perspectivas sobre la protección penal del software", en: *El cibercrimen, nuevo retos jurídico-penales, nuevas respuestas político criminales*, Comares, Granada, 2006, pp. 126-127.

Junto a las cuatro conductas anteriores se ha añadido en el art.270.1 CP con la reforma del pasado mes de marzo una cláusula abierta que establece que además de ellas también es punible toda conducta por la que *de cualquier otro modo explote económicamente* el objeto material del delito, véase el programa de ordenador o la base de datos en el caso de la ciberdelincuencia. De esta manera el artículo no reduce las conductas punibles a esas cuatro acciones concretas, (lo que podría generar problemas interpretativos o limitar las posibilidades a la hora de enjuiciar a los responsables de estos delitos), sino que amplía el alcance del precepto a cualquier otro supuesto que genere un beneficio económico al autor aunque no venga precedido por esas cuatro acciones específicas

Respecto a su tipo subjetivo se trata de un delito doloso que tradicionalmente ha requerido el ánimo de lucro para su consumación, (pues la conducta culposa no se prevé) y que se actuara en perjuicio de un tercero. Sin embargo en la actual redacción y como consecuencia de la citada reforma se ha introducido una frase que sustituye al ánimo de lucro, haciendo que el precepto amplíe su ámbito de aplicación de forma considerable. De este modo en la actual redacción en lugar de hacer referencia al ánimo de lucro se prevé el ***"ánimo de obtener un beneficio económico directo o indirecto"***.

> La razón de dicha sustitución se debe a que el requisito subjetivo del ánimo de lucro ocasionaba numerosos problemas interpretativos, pues la interpretación que se hacía de él era muy restrictiva, requiriendo que el lucro se consiguiera en la misma acción de forma directa. Ello generaba problemas en los casos en que el autor no se lucraba directamente con la conducta sino indirectamente, como por ejemplo a través de publicidad inserta en páginas web que reproducen material ilícito. De esta forma la conducta no se podía castigar al venir el beneficio económico de forma indirecta, lo cual hacía inexistente el delito. No obstante había sentencias donde a través del beneficio indirecto se integraba el ánimo de lucro consumándose el delito.
>
> También generaba problemas en el sentido contrario, es decir cuando la conducta era llevada a cabo por particulares que realizaban descargas ilícitas de contenidos para su reproducción particular por ejemplo. En tales casos al entender el ánimo de lucro como un ánimo comercial o de obtener un provecho económico la conducta quedaba impune, pues no se cumplía el tipo subjetivo. Ahora en cambio al tipificar el beneficio económico indirecto tales conductas quedan subsumidas en el ámbito subjetivo, pues la conducta de los particulares les evita tener que gastar dinero en la compra de la obra considerándose por tanto como un lucro indirecto.

> A mi juicio el nuevo tipo subjetivo es demasiado amplio e indeterminado, lo cual ocasionará problemas interpretativos pues al abarcar tantos supuestos una interpretación literal del mismo daría lugar a una tipificación de una multitud de acciones cotidianas con escasa trascendencia penal y con una mínima lesión del bien jurídico protegido (aunque en su conjunto podrían dañarlo), lo que vulneraria el principio de intervención mínima del Derecho penal. De ahí que la solución jurídica más coherente a la hora de aplicar el precepto sería tipificar los actos que ocasionen mayores perjuicios en los derechos de autor, incluyendo, ahora sí, la conducta de quien se lucra con la publicidad que introduce en las páginas dedicadas a vulnerarlos, y dejando fuera las conductas de escasa entidad que vengan llevadas a cabo por particulares para usos privados.

Con el cambio legislativo se facilita la aplicación del tipo al requerir el beneficio económico directo o indirecto, aunque como se ha visto ello amplía las conductas punibles.

Finalmente se exige que venga precedido de una acción en la que no haya un consentimiento del titular de los derechos de propiedad intelectual. En este sentido el consentimiento que haya prestado el titular de tales derechos conforme al régimen que integra el TRLPI, (un acto expreso e inequívoco), supondrá la atipicidad del hecho.

Tampoco sería punible la conducta realizada dentro de los límites establecidos, tanto temporales como materiales, a los derechos de explotación exclusiva[96]. Por ejemplo si la vulneración de estos derechos se produjera una vez que ha pasado el plazo en el que el TRLPI les protege, la conducta sería impune.

En cuanto al resto de párrafos que integraban el art.270.1 CP, la reforma de 2015 los ha suprimido, dejándolo solo en los términos que se han expuesto para así configurar el primer número del art.270 como el tipo básico en materia de propiedad intelectual. Tales párrafos han sido recolocados como a continuación se expondrá.

3.2 El tipo atenuado y los llamados manteros

El art.270.4 CP castiga las conductas de los vendedores ambulantes, los llamados *manteros*.

> *"En los supuestos a que se refiere el apartado primero, la distribución o comercialización ambulante o meramente ocasional se castigará con una pena de prisión de seis meses a dos años.*

[96] Véase más ampliamente MIRÓ LLINARES, F., *Internet y delitos contra la propiedad intelectual*, Datautor, Madrid, 2005, pp. 156-157.

> *No obstante, atendidas las características del culpable y la reducida cuantía del beneficio económico obtenido o que se hubiera podido obtener, siempre que no concurra ninguna de las circunstancias del artículo 271, el Juez podrá imponer la pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días".*

En el primer párrafo se rebaja la pena de estas conductas cuando sean llevadas a cabo de manera ambulante u ocasional; mientras que en el segundo se ha incluido en forma de delito leve lo que antes estaba previsto en el art.270.1.

> El supuesto original se encontraba en la anterior redacción dentro del tipo básico en el art.270.1, que introdujo la LO 5/2010[97] para permitir al juez rebajar la pena atendiendo al escaso beneficio económico y a las características del culpable, siempre que no se incurriera en alguna circunstancia agravante.
>
> Un supuesto similar era el que se contemplaba en el Libro III de las faltas de la anterior versión del Código Penal, pero al desaparecer con la última reforma ha sido necesario adaptarlas dando lugar su comisión al delito leve contemplado en el art.270.4.

En el precepto se atenúa la pena por una serie de circunstancias como son: la escasa entidad del delito; la distribución o comercialización ambulante o meramente ocasional; las características del culpable; y la reducida cuantía del beneficio económico obtenido o que se hubiera podido obtener. Se aplica por ejemplo en los supuestos de las personas que en la vía pública se dedican a la venta de películas obtenidas de forma ilícita.

El problema que tiene el precepto es su ambigüedad, pues no alude a cifras exactas a diferencia de otros delitos de este mismo Título como el de hurto, la estafa o la apropiación indebida en los que se fija la cifra de 400 euros para estar ante uno de esos delitos. Aquí en cambio se usan términos genéricos como la realización de la conducta "*meramente ocasional",* o "*atendida la reducida cuantía del beneficio económico"*, sin fijarla en una cifra concreta.

4. Aspectos comunes en los delitos contra la propiedad intelectual

En los números tercero, cuarto y quinto del art.270 CP se recogen una serie de conductas comunes a toda la regulación en materia de propiedad intelectual.

---

[97] Decía el artículo, *"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".*

4.1 Medidas cautelares y retirada de contenidos ilícitos en la red

En el art.270.3 CP se establecen las consecuencias de las conductas anteriores, facultando al juez a que retire los contenidos ilícitos de los servidores de Internet, e incluso pudiendo acordar el bloqueo del acceso a dicho portal.

> *"En estos casos, el juez o tribunal ordenará la retirada de las obras o prestaciones objeto de la infracción. Cuando a través de un portal de acceso a Internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos objeto de la propiedad intelectual a que se refieren los apartados anteriores, se ordenará la interrupción de la prestación del mismo, y el juez podrá acordar cualquier medida cautelar que tenga por objeto la protección de los derechos de propiedad intelectual.*
>
> *Excepcionalmente, cuando exista reiteración de las conductas y cuando resulte una medida proporcionada, eficiente y eficaz, se podrá ordenar el bloqueo del acceso correspondiente.".*

Al igual que sucedía en los números anteriores, el contenido íntegro del precepto ha sido dado por la LO 1/2015 estableciendo una serie de medidas que puede adoptar el juez para así mitigar las consecuencias económicas que producen estos delitos en los autores. De este modo se permite retirar todo el material ilícito de Internet e incluso cerrar las propias páginas web que realicen las conductas tipificadas en los artículos anteriores, (es decir el tipo básico recogido en el primer número y la conducta de las Webs de enlace del segundo).

A ello añade incluso la posibilidad de realizar medidas cautelares durante el transcurso del proceso, a fin de no tener que esperar a la sentencia y evitar que se sigan produciendo vulneraciones en los derechos de propiedad intelectual.

Tales facultades han sido añadidas en su totalidad por la nueva reforma penal, pues con anterioridad ninguna de ellas se preveía, al menos en lo que a la legislación penal respecta.

4.2 Importación, exportación y facilitación de las conductas que vulneran los derechos de propiedad intelectual

En art.270.5 CP se incluyen otras conductas como la importación, exportación o la facilitación del acceso. Tales conductas antes se encontraban en los apartados segundo y tercero del art.270.

> *"Serán castigados con las penas previstas en los apartados anteriores, en sus respectivos casos, quienes:*

> *a) Exporten o almacenen intencionadamente ejemplares de las obras, producciones o ejecuciones a que se refieren los dos primeros apartados de este artículo, incluyendo copias digitales de las mismas, sin la referida autorización, cuando estuvieran destinadas a ser reproducidas, distribuidas o comunicadas públicamente.*
>
> *b) Importen intencionadamente estos productos sin dicha autorización, cuando estuvieran destinados a ser reproducidos, distribuidos o comunicados públicamente, tanto si éstos tienen un origen lícito como ilícito en su país de procedencia; no obstante, la importación de los referidos productos de un Estado perteneciente a la Unión Europea no será punible cuando aquellos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento.*
>
> *c) Favorezcan o faciliten la realización de las conductas a que se refieren los apartados 1 y 2 de este artículo eliminando o modificando, sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, las medidas tecnológicas eficaces incorporadas por éstos con la finalidad de impedir o restringir su realización.*
>
> *d) Con ánimo de obtener un beneficio económico directo o indirecto, con la finalidad de facilitar a terceros el acceso a un ejemplar de una obra literaria, artística o científica, o a su transformación, interpretación o ejecución artística, fijada en cualquier tipo de soporte o comunicado a través de cualquier medio, y sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, eluda o facilite la elusión de las medidas tecnológicas eficaces dispuestas para evitarlo."*

El artículo añade pocas previsiones que no estuvieran en la redacción anterior, pero lo sistematiza de una forma más clara juntando lo que estaba en el segundo y tercer apartado en uno solo con cuatro letras en las que se distinguen mejor las conductas de importación, exportación, facilitación de tales conductas o la elusión de medidas tecnológicas que eviten tales comportamientos.

La LO 15/2003 fue la que dio una primera redacción a estos comportamientos y que hoy han vuelto a verse modificados mediante la LO 1/2015.

- En primer lugar se castiga la exportación o almacenamiento del objeto material protegido en los anteriores apartados, incluidas sus copias. Sin embargo añade un especial requisito dentro del ámbito subjetivo al requerir que las finalidades por las que se realiza la acción sean las de distribución, reproducción o comunicación.

  En cualquier caso la conducta debe producir una lesión en los intereses patrimoniales del autor y que derive de la distribución.

Además la misma letra incrimina el almacenamiento ilícito de dichas obras. Para que sea punible debe venir unido a la intención dolosa del autor de comerciar con ellas posteriormente, y que las propias obras sean ilícitas, pues como sucede en la exportación se requiere la finalidad de una posterior distribución, reproducción o comunicación.

- En segundo lugar se castiga la importación, siempre que tengan las mismas finalidades que las exigidas en la letra anterior. En este caso es indiferente que la conducta sea legal o ilegal en el origen desde el que se importa, ya que cuando acceden a territorio español la conducta es punible con independencia del origen. La única excepción es que procedan de un país europeo y en él la conducta haya sido legal, sólo en ese caso en España también lo será. En este sentido para que no sea punible se requiere que se hayan adquirido las obras del titular de los derechos en la Unión Europea o con su consentimiento. Ello es consecuencia de los principios básicos de la Unión al permitir la libre circulación, ya sea de personas, bienes o capitales.

  Las conductas anteriores habrá que ponerlas en relación con la de distribución del art.270.1, pues podría ser que quien lo almacena esté autorizado a la exportación o importación, pero no a su distribución, pues tal extremo no ha sido acordado con el autor.

- La tercera letra se refiere a quien favorezca o facilite la realización de las conductas de los dos primeros números, (tipo básico y atenuado) eliminando o modificando las medidas tecnológicas eficaces incorporadas por éstos con la finalidad de impedir o restringir su realización. De este modo se incrimina una modalidad específica de coautoría por la que se castiga la conducta de quienes de manera artificial consiguen eludir medidas previstas para que no se produzcan vulneraciones de los derechos de propiedad intelectual sobre la obra.

  El bien jurídico sigue siendo el mismo que en el resto de conductas, pero en este caso la naturaleza del injusto no es tan grave, pues lo que hace el legislador es adelantar la intervención penal, puesto que lo que se incriminan son actos preparatorios para un posterior ataque a los derechos de propiedad intelectual, es decir que no se llega a lesionar en un primer momento el bien jurídico de forma directa.

- Finalmente la última conducta alude al comportamiento de quien para facilitar a terceros el acceso a una obra protegida, eluda o facilite la elusión de las medidas tecnológicas eficaces dispuestas para evitarlo.

  Es muy similar a la letra anterior pero en lugar de realizar tales actos con la finalidad de permitir las clásicas conductas de reproducción, comunicación, distribución… se hace para permitir el acceso a los terceros a las obras.

Son conductas previas a que se lesione la propiedad intelectual ya que esos dispositivos lo que hacen es realizar otro tipo de acciones no directamente relacionadas con la vulneración de la propiedad intelectual sino facilitándolo en un momento posterior. Es por tanto una manera de adelantar las barreras de protección frente a acciones previas a la lesión de la propiedad intelectual. El peligro que se genera en ese momento es abstracto.

En este sentido para estar ante las conductas anteriores no es necesario haber realizado previamente los hechos tipificados en el art.270.1 CP, sino que basta con realizarlas aisladamente, aunque con la intención cometerlos posteriormente. Es decir que el origen de tales conductas no tiene porque ser siempre ilícito, sino que el ilícito sobreviene posteriormente.

En este supuesto la reforma busca dejar de lado el objeto típico de la regulación (obras literarias, artísticas o científicas) para regular otras conductas vinculadas de forma más lejana en indirecta con la propiedad intelectual. Todas ellas son dolosas que requieren el ánimo de obtener un beneficio económico directo o indirecto, o actitudes intencionales tendentes a vulnerar los derechos de propiedad intelectual sin la autorización del autor.

4.3 Fabricación, tenencia y puesta en circulación de dispositivos susceptibles de vulnerar los derechos de propiedad intelectual

Finalmente el art.270 CP se cierra con el número sexto en forma de delito de peligro al tipificar la fabricación, puesta en circulación o tenencia de productos que sirvan para realizar los ilícitos regulados en este artículo.

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

Se trata de medios que permiten eludir los sistemas de seguridad de los programas de ordenador o de las obras protegidas favoreciendo la realización del ilícito. Con ello se tipifica una forma concreta de ciberdelincuencia que está en la línea de la reforma que lo introduce, propensa a ampliar las barreras de protección penal a supuestos alejados a la vinculación más directa con el bien jurídico.

Con el artículo se castigan las creaciones de programas que facilitan la vulneración de los derechos de propiedad intelectual de forma indirecta, pues el delito se consuma con la mera creación de tales programas no con la vulneración de las obras. Estos programas no van destinados a dicha vulneración, sino a facilitar la supresión de dispositivos técnicos que protegen las obras de las conductas previstas en los tipos básico y atenuado de este artículo.

4.4 La responsabilidad civil derivada de los delitos contra la propiedad intelectual

Finalmente la regulación se cierra con el art.272 CP en el que se incluyen previsiones para determinar la responsabilidad civil que derive del delito. Para ello se remite a la legislación civil contenida en el TRLPI.

> *"La extensión de la responsabilidad civil derivada de los delitos tipificados en los dos artículos anteriores se regirá por las disposiciones de la Ley de Propiedad Intelectual relativas al cese de la actividad ilícita y a la indemnización de daños y perjuicios".*

Concretamente la remisión la hace a los art.139 y 140 TRLPI en los que se recogen las acciones relativas al cese de la actividad ilícita y a la indemnización de daños y perjuicios.

En cuanto a las primeras, el art.139 prevé una serie de conductas que comprenden el cese de la actividad ilícita[98] tendentes a evitar que el autor continúe con la conducta ilícita o que la reanude, así como la destrucción de los medios usados en la misma. Y por su parte el art.140 reconoce el derecho a una indemnización por daños y perjuicios al titular del derecho infringido, que comprenderá el valor de la pérdida que haya sufrido y el de la ganancia que haya dejado de obtener a causa de la violación de su derecho.

5. Agravantes

Las anteriores conductas se ven agravadas por el art.271 CP en atención a su mayor desvalor. Tales agravantes serán de aplicación una vez cometidas las conductas del art.270.

[98] El art.139 TRLPI contiene una serie de conductas que comprenden el cese de la actividad ilícita, entre ellas destacan, La suspensión de actividad infractora; la prohibición de reanudar la actividad infractora; la retirada del comercio de los ejemplares ilícitos y su destrucción; la retirada de los circuitos comerciales, la inutilización, y la destrucción de los moldes, planchas, matrices, negativos y demás elementos materiales, destinados a la reproducción, a la creación o fabricación de ejemplares ilícitos; la remoción o el precinto de los aparatos utilizados en la comunicación pública; el comiso, la inutilización y, la destrucción de los instrumentos, que faciliten la supresión o neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger un programa de ordenador; la remoción o el precinto de los instrumentos utilizados para facilitar la supresión o la neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger obras o prestaciones aunque aquélla no fuera su único uso; la suspensión de los servicios prestados por intermediarios a terceros para infringir derechos de propiedad intelectual.

> *"Se impondrá la pena de prisión de dos a seis años, multa de dieciocho a treinta y seis meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando se cometa el delito del artículo anterior concurriendo alguna de las siguientes circunstancias:*
>
> > *a) Que el beneficio obtenido o que se hubiera podido obtener posea especial trascendencia económica.*
> >
> > *b) Que los hechos revistan especial gravedad, atendiendo el valor de los objetos producidos ilícitamente, el número de obras, o de la transformación, ejecución o interpretación de las mismas, ilícitamente reproducidas, distribuidas, comunicadas al público o puestas a su disposición, o a la especial importancia de los perjuicios ocasionados.*
> >
> > *c) Que el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que tuviese como finalidad la realización de actividades infractoras de derechos de propiedad intelectual.*
> >
> > *d) Que se utilice a menores de 18 años para cometer estos delitos".*

Los cuatro supuestos ya se contemplaban con anterioridad a la reforma de una forma similar, pero ahora se añade algún cambio.

> Entre tales cambios encontramos que la letra a), que fundamenta la agravación en base al beneficio obtenido, ahora incluye que incluso cuando el autor no haya obtenido beneficio alguno se puede agravar ("*o se hubiera podido obtener").* De este modo la propia tentativa es agravada.
>
> El segundo apartado también difiere del de la anterior redacción al incluir nuevos supuestos en que se considera que los hechos revisten especial gravedad, como el número de obras producidas ilícitamente.

En las dos primeras conductas relativas a la trascendencia económica y a la gravedad del daño cabe señalar que no pueden ser cometidas mediante la conducta de reproducción, sino que por su propia naturaleza solo lo harán mediante la distribución, comunicación pública y plagio, (además de importación o exportación cuando luego tales conductas se lleven a cabo).

Junto a esas dos agravantes se alude también a la pertenencia a una organización que realice las actividades contempladas en los anteriores artículos, o que se hayan utilizado a menores de 18 años para cometer los hechos.

> La previsión acerca de la organización criminal tiene su relevancia en la sociedad actual al estar proliferando las organizaciones "piratas" que cuentan con estructuras perfectamente establecidas para llevar a cabo los ilícitos previstos en esta Sección.
>
> Y en relación a los menores sucede algo similar al ser usados frecuentemente por las mismas organizaciones y así cometer los ilícitos aprovechándose de su ausencia de responsabilidad penal en cuanto al Código Penal.

De tales agravantes se demuestra la importancia que revisten los hechos descritos, pues entre ellos se alude a la trascendencia económica que hayan generado las conductas para fundamentar la cualificación de la responsabilidad penal, ya que muchos de los aspectos protegidos constituyen una parte importante del progreso tecnológico y económico, los cuales de no estar severamente protegidos frente a su difusión masiva y gratuita desincentivarían a sus creadores a seguir progresando.

6. Las Webs de enlace

El número segundo del art.270 contempla un nuevo supuesto para hacer frente a una actividad que está de actualidad, la de las páginas web de enlace.

Estas son páginas webs que directamente no realizan ninguna conducta punible, pues ellas no reproducen, plagian, distribuyen o comunican públicamente obras protegidas, pero en cambio contienen enlaces ordenados que conducen a otras páginas donde sí que se realizan tales comportamientos.

> *"La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en Internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios".*

El artículo incide principalmente en el seno de los delitos informáticos, pues comprende conductas pensadas expresamente para ser cometidas por medio de Internet. Se trata de los comportamientos de páginas que contienen enlaces ordenados y clasificados, con información de su contenido y que conducen al usuario de manera sencilla e interactiva hacia terceras páginas en que se realizan los comportamientos del tipo básico del art.270.1 CP.

De este modo con el artículo se amplía la posibilidad de castigar no solo a quien realiza la vulneración directamente de la propiedad intelectual sino también a quien lo facilita. Está pensando en el supuesto de páginas web que ofrecen estos servicios (webs de enlace), ellas mismas no vulneran la propiedad intelectual pero ofrecen todo tipo de enlaces a películas, series o documentales de forma ordenada y con información acerca de ellas.

Antes de la reforma los tribunales habían descartado la relevancia penal de las Webs de enlace porque no infringían los derechos de autor, ya que estos son facultades personales que se reservan al titular de la obra y las páginas no eran titulares. Ahora con el cambio legislativo se permite que se les incrimine específicamente.

El artículo prevé para su consumación una conducta dolosa de la Web de enlace, pues requiere que *"facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico"*. Es decir debe tratarse de Webs en las que de manera explícita se publicite el contenido ilícito al que conducen sus enlaces, tales como series o películas, dando información de todas ellas. Ello se hace mediante listados clasificados y ordenados de todo el material que ofrecen, de forma que es verdaderamente sencillo para el usuario acceder al contenido ilícito.

Junto a ello es necesario, al igual que en el tipo básico, que estas webs actúen con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de un tercero. De nuevo ya no se habla del ánimo de lucro sino que basta con el ánimo de obtener un beneficio, tanto directo como indirecto, lo cual aumenta las conductas punibles al respecto.

Finalmente cabe señalar que el artículo no solo habla de facilitar el acceso a tales contenidos sino además la localización a los mismos. Ello provoca que no sea necesario llegar a acceder al contenido ilícito para que el delito se consume, pues con la mera localización basta.

La introducción de este supuesto es un paso más en la respuesta penal contra los delitos informáticos, ya que mediante él se extiende la protección contra todos aquellos autores que directamente no participan en su vulneración pero la facilitan proporcionando el acceso a la fuente de la que procede la lesión al derecho.

Por este motivo el tipo plantea problemas acerca de una posible vulneración del principio de lesividad al no haber un peligro directo para la vulneración del bien jurídico.

De este modo el art.270.2 CP se configura como delito de peligro abstracto, ya que la vinculación con el delito es muy lejana, genérica.

En este ámbito se solapa bastante el TRLPI que prevé mecanismos para que previamente a la vía judicial se actúe de manera administrativa. Ello favorece el principio de intervención mínima del Derecho penal, reservado para los casos más graves donde la lesión al bien jurídico no se puede reparar de otro modo.

Finalmente, para concluir esta cuestión cabe señalar que en líneas generales se trata de una reforma necesaria que expande y endurece la respuesta penal frente a todas estas conductas y que en muchos casos es útil e importante ya que las pérdidas en el sector de la propiedad intelectual son millonarias.

A ello se añade la facilidad que hay actualmente para vulnerar los derechos de autor en Internet, pues ahí se encuentran de manera rápida y sencilla multitud de páginas web que ofrecen todo tipo de contenidos que infringen la propiedad intelectual.

Sin embargo también cabe apreciar el considerable aumento de la tipicidad a conductas que en algunos casos no vulneran lo suficiente el bien jurídico como para entrar en el ámbito penal. Además en otros casos la conducta tipificada no está directamente relacionada con la lesión a la propiedad intelectual.

SECCIÓN QUINTA: **DELITOS CONTRA LA LIBERTAD SEXUAL. LA PROBLEMÁTICA DE MENORES Y PERSONAS CON DISCAPACIDAD NECESITADAS DE ESPECIAL PROTECCIÓN**

1. Introducción

La libertad sexual plantea serios problemas cuando las conductas que la vulneran se cometen mediante el uso de la red. Se trata de conductas en las que los autores se sirven del anonimato y de las posibilidades que ofrece Internet para crear una falsa identidad y con ello obtener favores sexuales y vulnerar la intimidad de sus víctimas. En definitiva, atentar contra su libertad sexual.

Por la propia naturaleza de los delitos sexuales en la red las víctimas suelen ser menores o **personas con discapacidad necesitadas de especial protección**[99]**,** ya que las acciones que se realizan en Internet si intervienen mayores de edad se convierten en lícitas,

[99] El término "incapaz" para el Derecho Penal es distinto que en otros ámbitos del Derecho como el civil. Tradicionalmente, para el Derecho penal por incapaz se entendía en el art.25 CP a "*toda persona, haya sido o no declarada su incapacitación, que padezca una enfermedad de carácter persistente que le impida gobernar su persona o bienes por sí misma"*. Esta precisión hay que tenerla muy en cuenta durante todo el estudio que nos ocupa, pues para el Derecho penal no es preciso que haya una sentencia civil para considerar a la víctima como incapaz. La trascendencia penal es enorme, pues numerosos tipos incluyen menciones hacia ellos, principalmente en forma de agravantes como sucede en los delitos contra la libertad sexual o la integridad física.
Sin embargo, como acabamos de señalar con la reforma del Código Penal introducida por la LO 1/2015, de 30 de marzo, se ha modificado dicho artículo para ampliar el significado de incapaz, expandiendo la discapacidad que deben padecer a nuevos supuestos. El nuevo artículo 25 señala, *"a los efectos de este Código se entiende por discapacidad aquella situación en que se encuentra una persona con deficiencias físicas, mentales, intelectuales o sensoriales de carácter permanente que, al interactuar con diversas barreras, puedan limitar o impedir su participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás. Asimismo a los efectos de este Código, se entenderá por persona con discapacidad necesitada de especial protección a aquella persona con discapacidad que, tenga o no judicialmente modificada su capacidad de obrar, requiera de asistencia o apoyo para el ejercicio de su capacidad jurídica y para la toma de decisiones respecto de su persona, de sus derechos o intereses a causa de sus deficiencias intelectuales o mentales de carácter permanente"*.
Introduce un matiz importante, pues el propio término se modifica y en lugar de hablar de "incapaces" se habla de "*personas con discapacidad necesitada de especial protección*". A continuación mantiene el requisito de que no es necesaria una sentencia judicial que lo avale, pues establece que no es necesario que se haya modificado su capacidad de obrar judicialmente. Además el término "minusvalía" le sustituye por "discapacidad", y en este mismo sentido los términos "minusválidos" y "personas con minusvalía", por "personas con discapacidad".
El Preámbulo de la reforma justifica dicho cambio para adecuar nuestra legislación a la Convención Internacional sobre los Derechos de las Personas con Discapacidad, hecha en Nueva York el 13 de diciembre de 2006 y así prevenir las conductas discriminatorias que puedan impedirles el disfrute de sus derechos en igualdad de condiciones. De este modo la totalidad del trabajo ha sido adaptada a tal cambio terminológico, hablando ahora de "personas con discapacidad necesitadas de especial protección" en lugar de "incapaces".

como sucede en los delitos de exhibicionismo y de corrupción de menores por ejemplo, en los que el hecho de distribuir material pornográfico o realizarle con mayores de edad y hacia ellos es perfectamente lícito. En cambio esa misma conducta con menores o personas con discapacidad necesitadas de especial protección se convierte en un delito tipificado en los artículos 185, 186 y 189.1 del Código Penal. Por este motivo el estudio de su regulación quedará orientado a los tipos penales específicos que les afectan en dicha materia.

Entre las conductas punibles destaca el acoso a menores y personas con discapacidad necesitadas de especial protección, conocido como *child grooming*, que ha sido recientemente reformado y ampliado en el art.183.ter. También se encuentran supuestos de corrupción con menores o personas con discapacidad necesitadas de especial protección, e incluso relativos a la elaboración de material pornográfico con ellos mismos.

Además hay otras conductas relativas a la vulneración de la libertad sexual y de otros derechos de menores y personas con discapacidad necesitadas de especial protección que se desarrollan específicamente en la red y que están cobrando importancia en los últimos años con el desarrollo de las nuevas tecnologías. Tales conductas son el *cyberbullying* (acoso entre jóvenes); *cyberstalking* (ciberacecho); *happy slapping* (filmación y distribución de la agresión sexual) y *sexting* (envío de material propio con contenido sexual).

El factor común de los citados comportamientos es que se realizan en Internet aprovechando las redes sociales y valiéndose de la virtualidad que permiten, facilitando el anonimato, la rápida distribución del material y el acceso al mismo por parte de una inmensa pluralidad de sujetos.

Todas las conductas están siendo ampliadas al mismo tiempo que con el desarrollo de la informática y de los dispositivos electrónicos van surgiendo nuevas modalidades delictivas.

2. Bien jurídico protegido

La importancia que revisten los citados comportamientos y por lo que se hace necesaria la intervención del legislador es por la vulneración que producen en la libertad sexual del sujeto pasivo en general, y en su indemnidad sexual en particular, relacionado este último caso cuando atentan contra menores y personas con discapacidad necesitadas de especial protección.

En primer lugar la **libertad sexual** se configura en nuestro ordenamiento como uno de los bienes jurídicos más sutiles de proteger, ya que el ámbito sexual está muy vinculado con la intimidad, y al igual que sucedía cuando tratábamos de delimitarla, depende mucho de la forma de ser de cada individuo así como de sus concepciones morales a las que se vincula la sexualidad.

En un sentido amplio la libertad se protege en el Título VI del Código Penal y en el art.17 de la Constitución. Pero debido a la importancia que revisten las conductas que la vulneran en su dimensión sexual, en el Título VIII del Código Penal aparecen comportamientos específicos en este ámbito bajo la rúbrica "delitos contra la libertad e indemnidad sexuales", siendo una modalidad de los delitos contra la libertad.

La libertad sexual según MUÑOZ CONDE[100] se entiende como *aquella parte de la libertad referida al ejercicio de la propia sexualidad y, en cierto modo, a la disposición del propio cuerpo, configurada como un bien jurídico merecedor de una protección penal específica, no siendo suficiente para abarcar toda su dimensión con la protección genérica que se concede a la libertad.*

La libertad sexual goza de una autonomía propia en el Código al orientarse a castigar los ataques violentos o intimidatorios contra el ejercicio de la sexualidad, como sucede en los delitos de agresiones y abusos sexuales.

Junto a la libertad sexual se introdujo en la reforma del Código Penal de 1999 un nuevo bien jurídico, la **indemnidad sexual**. Con la reforma se posibilitaba la inclusión de nuevos tipos penales que se alejaban del ámbito de aplicación estricto de la libertad sexual y más vinculados a menores y personas con discapacidad necesitadas de especial protección, donde lo que se buscaba era proteger las conductas que podían afectar a la evolución y desarrollo de su personalidad, y producir en ella alteraciones importantes que incidan en la vida o en el equilibrio psíquico del menor en el futuro. Se persigue que el menor pueda evolucionar y desarrollar su personalidad de manera normal y libre, para que así cuando sea adulto pueda decidir en libertad su comportamiento sexual[101].

Entre los comportamientos que vulneran la indemnidad sexual de los menores y de las personas con discapacidad necesitadas de especial protección destacan los delitos de

[100] MUÑOZ CONDE, F., *Derecho Penal parte especial,* Tirant lo Blanch, Valencia, 2010, pp. 216-217.
[101] Véase GARCÍA ÁLVAREZ, P., "El menor como sujeto pasivo de delitos, con especial referencia a los delitos contra la libertad e indemnidad sexual y los cambios en ellos introducidos por el proyecto de Ley Orgánica de 20 de septiembre de 2013", *Revista General de Derecho Penal,* 2013, pp. 18-19.

exhibicionismo, de elaboración o difusión de pornografía infantil, de corrupción de menores o personas con discapacidad necesitadas de especial protección y de prostitución.

En tales conductas no se habla de la libertad sexual, al carecer los sujetos de ella mientras sean menores o personas con discapacidad necesitadas de especial protección. De ahí que para garantizar su pleno desarrollo haya sido necesario acudir a este nuevo bien jurídico que de cobertura a tales situaciones.

En el caso de las personas con discapacidad necesitadas de especial protección la indemnidad sexual no se regula de la misma forma que con los menores al no estar su situación predeterminada por la edad sino por las condiciones de cada uno, (que serán las que le permitan a nivel intelectual tener un mayor o menor grado de discernimiento respecto del acto sexual), y por su facultad volitiva para consentirle.

3. Regulación penal. Menores y personas con discapacidad necesitadas de especial protección como sujetos pasivos del delito

La Constitución española en su artículo 39 otorga una amplia protección a la familia, pero específicamente a los menores como se desprende de los apartados segundo, tercero y cuarto de ese mismo artículo.

Las personas con discapacidad necesitadas de especial protección también quedan protegidas por mandato del art.49 CE al conculcar a los poderes públicos la tarea de prevenir, tratar, rehabilitar e integrar su situación. La especial vulnerabilidad que sufren debe orientar las políticas del Gobierno y de la Administración para reducir las limitaciones a las que se ven abocados en su vida diaria.

En este sentido y como consecuencia del compromiso adquirido en aras de reforzar la protección a los sujetos más vulnerables como son los menores y las personas con discapacidad necesitadas de especial protección, la reforma del Código Penal de este año ha introducido un cambio terminológico importante, pues como se ha señalado antes, todas las referencias del Código en que aparecía la palabra "incapaces" ahora pasan a denominarse "personas con discapacidad necesitada de especial protección", cualquiera que fuera el ámbito en que apareciesen.

La protección no puede ser menor desde el punto de vista del Derecho penal. A lo largo del Código se pueden apreciar las continuas referencias en forma de agravantes

cuando los menores y las personas con discapacidad necesitadas de especial protección son los sujetos pasivos de los distintos tipos.

> Ello sucede por ejemplo en el art.148 en el ámbito de las lesiones en sus números tercero y quinto cuando la víctima sea un menor o persona con discapacidad necesitada de especial protección y especialmente si convive con el autor; en el art.165 referido a los delitos de detención ilegal y secuestro que agrava la pena cuando sea un menor o una persona con discapacidad necesitada de especial protección; en los supuestos de delitos contra la salud pública cuando se trata del narcotráfico en el art.369.1.4 para el caso de que se suministren drogas toxicas, estupefacientes o sustancias psicotrópicas hacia menores de dieciocho años; conductas como la trata de seres humanos (art.177.bis.4b); el tráfico ilegal de personas (art.318.bis.2) que también otorga una especial protección a dichos sujetos; e incluso en ámbitos más cercanos a ellos como sucede en los delitos contra los derechos y deberes familiares, tal y como se desprende de los art.223 a 233.

Como se observa, las referencias a menores y a personas con discapacidad necesitada de especial protección son continuas en el Código, que consciente de su especial vulnerabilidad las recoge en numerosos tipos para garantizar su protección. El Derecho penal debe proporcionar la respuesta adecuada cuando dichos sujetos sean víctimas de algún delito para que no queden impunes y para prevenir que tales comportamientos no se vuelvan a repetir.

En el caso de los ciberdelitos la respuesta del Derecho penal no puede ser distinta, incluso debe ser más enérgica en atención a las especiales singularidades que presentan las conductas por las que se llevan a cabo, es decir el anonimato del que se sirve el autor, la máxima difusión del material ilícito en la red y las dificultades para encontrar al responsable. Además en los delitos en que las víctimas son menores o personas con discapacidad necesitadas de especial protección se producen especiales circunstancias debido a su vulnerabilidad y al mayor reproche que ocasionan en la sociedad.

Pero al mismo tiempo, la solución que se da a los ciberdelitos en el ámbito de la libertad sexual, tan vinculado con personalidad de las víctimas, no es la misma que cuando intervienen mayores de edad, debido al carácter que presentan los menores y las personas con discapacidad necesitadas de especial protección al no haber alcanzado su plena madurez física y mental y estar bajo la dependencia de sus padres, tutores o curadores. Ello hace que tales delitos se traten con una especial sensibilidad, pues las secuelas que quedan en ellos les pueden marcar el resto de la vida.

En este entorno es en el que se desarrollan los delitos informáticos contra la libertad sexual, ya que al requerir que la conducta se realice por medio de Internet, los supuestos quedan reducidos a acciones tendentes a engañarlos para así obtener favores sexuales o a comerciar con ellos mediante actos de pornografía infantil o similar.

En nuestro Derecho interno la regulación en materia de delitos informáticos contra la libertad sexual se encuentra recogida en el Título VIII del Libro II del Código Penal, entre los artículos 178 y 194[102]. En ellos se desglosan a lo largo de sus diferentes capítulos las conductas que atentan contra la libertad sexual y contra la indemnidad sexual en los términos antes comentados.

Sin embargo no todo el Título es de aplicación en los delitos informáticos, pues solo tres de sus múltiples conductas cumplen los requisitos que dan lugar a uno de ellos, es decir que se realicen por medio de la red o en general a través de una tecnología de la información y la comunicación.

Tales conductas son por un lado el delito de *child grooming,* es decir contactar con personas menores de 16 años (13 en la anterior redacción) para así ganarse su confianza y poder realizar relaciones sexuales. Este delito se encuentra tipificado en los art.183.bis, ter y quater; además encontramos el delito de exhibicionismo y provocación sexual recogido en los art.185 y 186; y el delito relativo a la corrupción de menores del art.189, en el que se incluyen todos los supuestos de pornografía infantil.

Todos estos tipos penales en materia de libertad sexual en la red y en especial los introducidos con la última reforma de 2015 han quedado afectados por dos instrumentos internacionales que han hecho necesaria su adaptación.

Se trata en primer lugar del Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual infantil de 25 de octubre de 2007, (conocido como el Convenio de Lanzarote). Fue ratificado por España en marzo de 2009

[102] En este sentido cabe llamar la atención sobre la reforma del Código Penal introducida por la Ley Orgánica 1/2015, de 30 de marzo, que será abordada con posterioridad. La reforma ha modificado sustancialmente toda esta materia, sobre todo en lo que se refiere a menores y a personas con discapacidad necesitadas de especial protección. Los cambios son a nivel general en todo el Capítulo, pero en el ámbito de la ciberdelincuencia destacan las modificaciones del art.183 en materia de acoso sexual a menores, al elevar la edad mínima para consentir mantener relaciones sexuales, y del art.189 sobre corrupción de menores, al prever nuevos supuestos punibles y dar un nuevo significado de pornografía infantil a efectos del Código Penal.

pero algunas de las propuestas que incluye han sido incorporadas en la reforma de 2015 del Código Penal[103].

El texto incluye una serie de conductas que ya forman parte de nuestro derecho interno desde antiguo, aunque ciertas modalidades no, lo que propició las reformas. Entre ellas destacan el *grooming,* la corrupción de menores, la prostitución de menores y la pornografía con los mismos, así como los abusos sexuales con ellos. Además recomienda la creación de programas educativos en materia sexual e incluye un régimen sancionador que incluye una serie de circunstancias agravantes, todas ellas ya previstas en nuestra legislación interna.

Todas las directrices han tenido que ser incorporadas al ordenamiento jurídico español tras la ratificación por parte de España del Convenio, lo que la convierte en parte del mismo obligándola a cumplir lo establecido en él.

Junto al Convenio destaca la Directiva 2011/93/UE de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales, la explotación sexual de los menores y la pornografía infantil.

Mantiene el mismo contenido que en Convenio y en este caso al tratarse de una Directiva comunitaria España queda obligada a transponerla a su ordenamiento, tarea que realizó con la reforma de 2015 en lo no previsto al respecto.

3.1 Delito de acoso a menores de 13 años, "child grooming". El aumento de la edad de consentimiento sexual

El delito de acoso sexual a menores o *child grooming* se encuentra regulado en el art.183.bis, que ha sido ampliado mediante la Ley Orgánica 1/2015[104] que reforma el Código Penal al añadir los art.183.ter y quater en los términos que a continuación se exponen.

En síntesis la conducta punible básica que recogía el art.183.bis consiste en la realización por parte de un adulto (aunque nada impide que la realice un menor) de propuestas por medio de las tecnologías de la información y la comunicación a un menor que no ha alcanzado la edad de consentimiento sexual relativas a encontrarse con él con el fin de realizar actos de carácter sexual con dicho menor o de producir pornografía infantil.

[103] http://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-17392
[104] http://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3439.pdf

La redacción original del tipo se introdujo en nuestro ordenamiento en el año 2010, mediante la Ley Orgánica 5/2010 como consecuencia del citado Convenio de Lanzarote en cuyo art.23 se preveía tal conducta.

Junto a ella en la reforma del año 2015 se ha ampliado el precepto mediante la inclusión de los art.183.ter y quater para dar cabida a nuevas exigencias internacionales, (entre las que destaca la Directiva también antes citada 2011/93/UE), a la vez que para resolver el problema de la pedofilia en la red. En este sentido, como es sabido en los últimos tiempos los pederastas han sustituido las visitas a los parques por los ordenadores, donde encuentran una facilidad mayor para llevar a cabo sus conductas sexuales al poder ocultar su verdadera apariencia logrando una confianza mayor con la víctima.

Como consecuencia de dicha reforma el orden del articulado se alteró pasando el tipo básico del art.183.bis[105] al art.183.ter. Será por tanto por este último por el que comenzará el estudio del primer delito informático en materia de libertad sexual.

El art.183.ter establece:

> *"El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 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".*

La conducta consiste en la utilización de las tecnologías de la información y la comunicación, (como una red social por ejemplo) con fines sexuales con menores. Para ello

[105] Como consecuencia de la reforma en la actualidad el art.183.bis contempla un supuesto que se aleja del ámbito del grooming y de la ciberdelincuencia en general, pues recoge una conducta específica relativa a la corrupción de menores que se solapa con la figura del abuso sexual.
En el artículo se castiga la conducta de quien determine a un menor de 16 años a participar en actos sexuales o le haga presenciarlos. Como se ve no pertenece al ámbito de la ciberdelincuencia más allá de posibles comportamientos en el caso de que el autor le hiciera presenciarlos mediante Internet u otra tecnología de la información y la comunicación. Sin embargo ello queda ya protegido en el capítulo relativo a los delitos de exhibicionismo y provocación sexual. La anterior redacción de esta conducta se tipificaba en el art.189.5 con un contenido diferente al hablar de "determinar" en lugar de "hacer participar" y además ya no se alude a que el comportamiento tenga que suponer un perjuicio para la evolución del menor.
Por ello con la nueva redacción se amplía el ámbito de aplicación dando lugar a un delito de peligro abstracto, ya que lo que se viene a castigar ya está contemplado en el art.185 mediante los delitos de exhibicionismo.

el autor se sirve de dicho medio y así ganarse la confianza de la víctima pudiendo obtener de una forma sencilla el encuentro sexual.

El sujeto activo del delito puede serlo cualquiera, incluido un menor si supera los 14 años de edad, al ser esta la edad mínima de responsabilidad penal como indica la Ley Orgánica de responsabilidad penal del menor en su artículo primero. Para ello habrá que estar a la relación entre autor y víctima y observar la regla del art.183 quater a la que posteriormente nos referiremos, (exime de responsabilidad penal al autor cuando tenga una cercanía en cuanto a madurez y edad con la víctima además de mediar un consentimiento libre, por lo que no será igual que la víctima tenga 13 años y el autor 17, a que tengan 15 y 17 años respectivamente).

El sujeto pasivo del delito debe ser un menor de 16 años, lo que ha supuesto una de las principales novedades de la reforma que ha introducido la LO 1/2015, no solo en materia de delitos sexuales sino a nivel global al elevar la edad de consentimiento sexual de los 13 a los 16 años.

> Por **edad de consentimiento sexual** se entiende aquella franja de protección absoluta de los menores frente a abusos sexuales, de modo que por debajo de esa edad no se concede relevancia alguna al consentimiento que el menor pueda prestar a la relación[106]. Se considera que por debajo de esa edad el consentimiento es ineficaz de manera *iuris et de iure.*
>
> El hecho de que se aumente la edad de consentimiento sexual supone que una relación sexuales que se tenga con un menor de 16 años da lugar a un delito de abusos sexuales, pues aunque hayan consentido el Derecho penal no otorga validez a dicho consentimiento al entender que los menores o las personas con discapacidad necesitadas de especial protección no pueden disponer sobre el bien jurídico protegido en los delitos contra la libertad sexual[107].
>
> De este modo no solo son constitutivos de delito los actos de contenido sexual realizados con violencia o intimidación, sino que hasta los 16 años no se otorga relevancia al consentimiento que pueda prestar un menor al entender que la relación sexual con él mantenida no ha sido consentida o no lo fue válidamente[108].

[106] ROPERO CARRASCO, J., "Reformas penales y política criminal en la protección de la indemnidad sexual de los menores", *Estudios penales y criminológicos, vol. XXXIV,* 2014, p.258.
[107] RUEDA MARTÍN, M. A., "La relevancia penal del consentimiento del menor de edad en relación con los delitos contra la propia imagen", *Revista para el análisis del Derecho,* 2013, pp. 20 y 30.
[108] GARCÍA ÁLVAREZ, P., "El menor como sujeto pasivo de delitos, con especial referencia a los delitos contra la libertad e indemnidad sexual y los cambios en ellos introducidos por el proyecto de Ley Orgánica de 20 de septiembre de 2013", *Revista General de Derecho Penal,* 20 (2013), p.19.

El legislador niega relevancia al consentimiento que pueda prestar en este ámbito todo menor de 16 años de edad, haciendo por ello que la relación sexual mantenida con el mismo sea constitutiva de delito por el simple hecho de haberla tenido. Una situación idéntica pero en la que interviniera un mayor de edad sería legal al poder consentir eficazmente.

Sin embargo con la citada reforma de 2015 la presunción por la que se considera ineficaz el consentimiento de un menor de 16 años en materia sexual ha dejado de ser *iuris et de iure* para ser de carácter *iuris tantum*, es decir admitiendo prueba en contrario, pues al mismo tiempo que se eleva la edad de consentimiento sexual, se introduce el art.183.quáter por el que se otorga validez al consentimiento expresado de manera libre cuando el autor sea próximo a la víctima por edad y grado de desarrollo o madurez.

La redacción anterior mantuvo la edad de consentimiento sexual en los 13 años, pero la trascendencia jurídica que tuvo fue escasa más allá de la repercusión acaecida en la doctrina, pues pocas sentencias condenaron a los autores por delitos relacionados con proposiciones sexuales telemáticas a menores. En este sentido la mayoría de los procesos terminaron en absolución de este delito concreto, en algún supuesto por error de tipo del autor acerca de la edad de la menor (Sentencia de la Audiencia Provincial de Valencia núm. 722/2013, de 24 de octubre) donde al no estar prevista su comisión culposa queda impune; y en otros por aplicación del principio de consunción del Derecho penal que implica considerar que el injusto del delito de *child grooming* quede englobado en el de abusos sexuales, quedando impune por tanto el primero (Sentencia de la Audiencia Provincial de Sevilla núm. 465/2013, de 3 de octubre).

Con la reforma se adecúa la protección penal a los menores frente a las nuevas conductas que están surgiendo en el seno de las nuevas tecnologías. El aumento de la edad de consentimiento sexual contribuirá seguramente a ampliar el número de conductas delictivas en este ámbito, ya que la mayoría de menores que mantienen relaciones sexuales no tienen la suficiente madurez a la hora de consentirlas y a lo que en principio pueden estar dispuestas, en un momento posterior se acaben arrepintiendo presentando la correspondiente denuncia alegando la falta de consentimiento. Por este motivo se entiende que los menores no pueden disponer de su sexualidad, al menos con personas que difieren respecto de ellos en cuando a edad y madurez, lo que les coloca en una posición de inferioridad.

Además el tipo no menciona a las personas con discapacidad necesitadas de especial protección como sujetos pasivos del mismo. Es una ausencia llamativa al estar bastante presentes en la mayoría de preceptos de este ámbito.

El bien jurídico protegido es la indemnidad sexual de los menores, en relación al normal desarrollo y formación de la vida sexual, o el derecho a no sufrir daño en la esfera sexual.

El delito se configura como de peligro abstracto, pues adelanta las barreras de protección penal a un momento anterior al de su realización. En realidad incrimina unos actos preparatorios del delito de abusos sexuales aunque con un matiz concreto, que se lleven a cabo por medios telemáticos y que la víctima no llegue a los 16 años de edad.

El desarrollo de la conducta típica se lleva a cabo mediante tres fases claramente diferenciadas[109]:

- En la primera de ellas el autor entabla contacto con el menor, de tal modo que no solo bastará con enviarle un mensaje, sino que el menor deberá responderle. El cauce por el que se realizará será necesariamente una tecnología de la información y la comunicación como Internet o una aplicación de mensajería instantánea para dispositivos móviles como Whatsapp por ejemplo.

  Con un solo mensaje bastaría para que este requisito se cumpliera, (siempre que hubiera respuesta por parte del menor), no tendría porque haber una reiteración de mensajes del autor en este sentido. En caso de que no haya respuesta por el menor no debería tomarse en cuenta ni siquiera como tentativa, pues no ha llegado a generarse el peligro, ya que como se ha señalado antes estamos ante actos de preparación del delito de abusos sexuales elevados a la consideración de delito.

- En segundo lugar, los actos que realiza el autor cuando entabla el contacto con el menor deben ir orientados a acercarse a él y así ir ganándose su confianza. Todos ellos deben ir tendentes a un ulterior contacto físico de carácter sexual, pues de lo contrario los actos quedarían encuadrados en supuestos de conspiración, proposición o provocación.

  En este elemento concurre la agravante que prevé el último inciso del artículo pues las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño. Este inciso es controvertido pues en la

[109] VILLACAMPA ESTIARTE, C., "Propuesta sexual telemática a menores u online child grooming: configuración presente del delito y perspectivas de modificación", *Estudios Penales y Criminológicos, vol. XXXIV*, 2014, pp. 682-693.

mayoría de los casos habrá engaño, y por tanto la agravante está implícita en el tipo básico.

- Finalmente el tercer elemento que cierra la conducta es que el fin con el que se lleva a cabo sea el de cometer los delitos de los artículos 183 y 189, es decir el de abusos sexuales a menores de 16 años y el de corrupción de menores respectivamente.

  En relación a la anterior redacción se ha suprimido la mención al art.178 constitutivo del tipo básico de agresiones sexuales como fin del delito. Y en cuanto a la mención del art.189 se generan dudas, ya que se omite la referencia a la prostitución de menores que se tipifica en el mismo capítulo pero en el nuevo art.188. De este modo se entiende que la exigencia de que el fin sea el del art.189 viene reducido a que la finalidad sea la de cometer actos encaminados a la agresión, abuso o captación y utilización del menor para elaborar material pornográfico o para hacerlo participar en espectáculos exhibicionistas o pornográficos del art.189.1.a)[110].

  Este elemento finalista es imprescindible ya que es el que provoca que se castigue el *grooming* en cuanto a acto preparatorio de un delito contra la indemnidad sexual.

  Cuando la finalidad perseguida por el autor sea otra como la de obtener material pornográfico del menor, entrará en aplicación el siguiente párrafo del art.183.ter que posteriormente se analizará. De ahí que el elemento intencional sea imprescindible para calificar la conducta y poder apreciar la comisión de este delito en grado de tentativa o simplemente que sea impune.

Junto a los actos por los que se lleva a cabo la conducta debe concurrir en todo momento el dolo de realizar el acto sexual con el menor. De realizar la acción de forma culposa, es decir sin saber que la víctima no alcanza los 16 años de edad y siendo ese error invencible o incluso vencible, por aplicación de las reglas generales del art.14.1 CP la conducta quedaría impune al no estar prevista su comisión culposa.

Para la consumación del delito no se necesita que llegue a existir el contacto sexual, incluso el menor no tiene ni que llegar a verse físicamente con el autor. Esto es que el

[110] En este sentido véase MUÑOZ CONDE, F., *Derecho Penal Parte Especial*, Tirant lo Blanch, Valencia, 2010, p. 240.

delito se consuma una vez que ambos sujetos han contactado y el autor ha propuesto una cita para en ella realizar la actividad sexual[111].

Finalmente las penas que se apliquen serán sin perjuicio de las correspondientes en su caso a los delitos cometidos, aunque por aplicación de las reglas de resolución del concurso, y en especial la de consunción o alternatividad, el delito más grave suele ser por el que se condena al autor.

A continuación el legislador introduce un nuevo párrafo al art.183.ter para castigar la conducta de embaucamiento.

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

Se trata de un delito relativo a la producción de pornografía infantil por la que mediante una tecnología de la información y la comunicación el autor contacta con un menor de 16 años, (y por tanto que no ha alcanzado la edad de consentimiento sexual) para embaucarle y obtener material pornográfico como fotos o videos.

Es un supuesto en el que se adelanta la barrera de protección penal a conductas que tienen más que ver con la pornografía infantil tipificada en el art.189. La pornografía no obstante no viene referida a que sea realizada por un tercero como sucede en el art.189, sino que es auto producida por el propio menor, ampliándose de este modo el número de conductas y situaciones punibles.

La cláusula relativa al material pornográfico es abierta, por lo que engloba cualquier tipo de material en el que no tiene que aparecer ni el propio menor.

Como se ha apuntado antes, la conducta citada trae como novedad el aumento de la edad sexual para consentir mantener relaciones sexuales a los 16 años, de tal modo que por debajo de dicha cifra aunque la víctima haya consentido de manera libre tenerlas no tiene validez para el Derecho penal.

La conducta además quedará exenta de responsabilidad cuando entre en aplicación el art.183.quater en los términos que posteriormente se expondrán.

---

[111] CUERDA ARNAU, M. L., "Menores y redes sociales: protección penal de los menores en el entorno digital", *Cuadernos de Política Criminal, núm. 112, I, Época II,* 2014, pp.28-29.

El problema del artículo es la proximidad con el art.189, cuyo ámbito de aplicación puede solaparse al referirse tanto a la captación de menores como a la producción de pornografía infantil.

Finalmente la reforma en el ámbito del *grooming* se cierra con la introducción del art.183.quater, configurándose como un contrapeso frente al aumento de la edad sexual para consentir mantener relaciones sexuales a los 16 años.

Según dicho artículo las conductas señaladas con anterioridad quedan exentas de responsabilidad penal cuando medie el consentimiento libre de la víctima y el autor sea próximo a ella en cuanto a edad y madurez o grado de desarrollo.

El artículo se introduce al ser consciente el legislador de que el ser humano es diferente entre sí y no se puede teorizar en una cifra concreta la posibilidad de consentir o no mantener relaciones sexuales.

> *"El consentimiento libre del menor de dieciséis años excluirá la responsabilidad penal por los delitos previstos en este Capítulo, cuando el autor sea una persona próxima al menor por edad y grado de desarrollo o madurez".*

Al aplicar este precepto los supuestos contemplados con anterioridad dejan de ser típicos, excluyendo la responsabilidad criminal tanto de mayores como de menores de edad por los hechos que en ellos se describen, siempre que se cumplan los requisitos que el artículo prevé. Es una excepción a la ineficacia que el Derecho penal otorga por lo general al consentimiento de un menor de 16 años.

Los requisitos que exige el artículo para que el consentimiento sea válido son que exista una proximidad entre el autor y la víctima en cuanto a tres aspectos, edad, grado de desarrollo y madurez, a lo que se añade que medie el consentimiento libre del menor de 16 años.

El problema que ocasiona la cláusula es que es demasiado abierta, pues no parece fácil determinar cuándo entre una persona de 15 años y otra de 17 hay proximidad en cuanto a la madurez por ejemplo. Por ello la interpretación no parece sencilla, debiendo hacerse de manera restrictiva de forma que ocasione la menor vulneración de derechos.

3.2 Delitos de explotación sexual de menores y personas con discapacidad necesitadas de especial protección en la red. Corrupción de menores y personas con discapacidad necesitadas de especial protección. El concepto de pornografía infantil

En el Capítulo V del Título VIII del segundo Libro del Código Penal se regulan los delitos relativos a la prostitución, a la explotación sexual y a la corrupción de menores y personas con discapacidad necesitadas de especial protección, entre otras conductas punibles. Tales conductas se desarrollan entre los artículos 187-189, siendo los dos primeros relativos a la prostitución de mayores y menores de edad, y el último sobre corrupción y explotación sexual de menores.

La relevancia jurídico penal para el ámbito de la delincuencia informática la tienen las conductas que se desarrollan en el art.189 sobre la pornografía infantil y el uso que se hace de menores y personas con discapacidad necesitadas de especial protección para producirla o para explotarlos en espectáculos de carácter sexual, pues la mayoría de esos contenidos vienen difundidos por medio de Internet donde se albergan multitud de páginas web que incluyen una gran variedad del citado material[112].

El bien jurídico protegido[113] en estas conductas es la protección de la educación en el ejercicio de la sexualidad y el rechazo a que menores y personas con discapacidad necesitadas de especial protección sean convertidos en objeto o mercancía para satisfacer el deseo sexual de terceros. Se trata de un ámbito en el que el menor o la persona con discapacidad necesitada de especial protección es tratado como un objeto sexual al que se explota, generando un enriquecimiento patrimonial en el autor a la que vez que se lesiona la indemnidad sexual de las víctimas.

En las conductas que se regulan en este ámbito en relación a los menores, (a diferencia de lo que sucedería si son llevadas a cabo por mayores), no es preciso que se

[112] Junto a la corrupción de menores el Capítulo alude a la prostitución de mayores, menores y personas con discapacidad necesitadas de especial protección pero que queda fuera del ámbito propio de la ciberdelincuencia. En relación a mayores de edad destaca que en nuestro ordenamiento jurídico la prostitución ejercida de manera libre por personas mayores de edad en sí misma no es delito, sino que lo que se castigan son ciertas conductas relacionadas con la misma, que son las de terceros que obligan principalmente a mujeres y niñas a ejercerla. En cuanto a los menores y a diferencia de lo que sucede con los mayores de edad, la prostitución ejercida por ellos sí que es constitutiva de delito en sí misma, aunque lo realicen de forma voluntaria sin violencia o coacción por parte de terceras personas, e incluso se castiga a quienes solicitan dichas relaciones.

[113] MUÑOZ CONDE, F., *Derecho Penal Parte Especial*, Tirant lo Blanch, Valencia, 2010, p. 253.

produzca un ataque contra su libertad, es decir que aunque se realicen de forma libre y consentida constituirán un delito por sí mismo.

El sujeto activo común a todas ellas es quien realiza la acción, en algunos casos será quien elabora el material pornográfico o capta a menores para realizarlo y en otros las personas que distribuyan ese material. Incluso también podrán serlo quienes ostenten la patria potestad, tutela, guarda o acogimiento de menores o personas con discapacidad necesitadas de especial protección y no impidan que desarrollen dichas conductas a pesar de tener conocimiento de las mismas.

Además todas las conductas punibles en este ámbito requieren el dolo del autor, es decir que actúe con conocimiento de que las personas que están realizando la actividad delictiva son menores o personas con discapacidad necesitadas de especial protección, pues como se ha indicado antes, la misma conducta llevada a cabo por mayores de edad quedaría exenta de responsabilidad penal. En este sentido al no estar prevista la comisión culposa de los tipos penales recogidos en el art.189, de ser realizados mediante error vencible o invencible en cuanto a la edad o incapacidad de las víctimas, la conducta quedaría impune, (art.14 CP).

Sin embargo aunque en el aspecto subjetivo todas estas conductas requieran un dolo directo nada impide que puedan ser cometidas mediante un dolo eventual. Es decir, aunque una conducta culposa del autor en cuanto a la edad de la víctima diera lugar a la exención de la responsabilidad penal, si su actitud no ha sido diligente a la hora de comprobar dicha edad, o actuó con indiferencia hacia la misma dándole igual si la víctima era mayor o menor, capaz o incapaz, el tipo podría ser cometido mediante dolo eventual[114].

Las **conductas delictivas** específicas relacionadas con la corrupción de menores en el entorno de la ciberdelincuencia, se recogen en el art.189 que ha sido afectado por la reforma introducida por la Ley Orgánica 1/2015.

El primer comportamiento delictivo que forma el tipo básico del delito se regula en la letra a) del primer apartado del art.189 en relación al uso de menores y personas con discapacidad necesitadas de especial protección en la elaboración de material pornográfico, y su utilización en espectáculos exhibicionistas o pornográficos.

[114] MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, p.124.

Comprende por tanto dos conductas, la de captar o utilizar a menores o personas con discapacidad necesitadas de especial protección para participar en espectáculos exhibicionistas o pornográficos; y la de elaborar con ellos mismos material pornográfico. A estas dos conductas que forman el tipo básico se incluye la de quien financie o se lucre con cualquiera de ellas.

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

Los medios para cometer cualquiera de los supuestos son comunes, entre ellos destaca el de "captar" a dichos sujetos, pues de ese modo se consigue adelantar la protección penal a momentos anteriores a su utilización en la elaboración del material pornográfico o su participación en los mismos[115]. Además con el término "captar" se amplían los supuestos en que el artículo se puede aplicar, llegando a multitud de actos preparatorios que van más del verdadero injusto que tienen tales conductas, como la participación física del menor o persona con discapacidad necesitada de especial protección en actos o espectáculos de contenido sexual y la elaboración con ellos mismos de material pornográfico, pero cuando mantienen dicha condición[116].

Al hecho de captar y utilizar menores el tipo penal añade como forma de realizarle la de financiar tales actividades lucrándose con los beneficios que generen.

- En cuanto a la primera conducta, la **captación o utilización** de menores o personas con discapacidad necesitadas de especial protección con fines exhibicionistas o pornográficos, cabe señalar que no requiere como forma de comisión que el material que se elabore sea pornográfico, sino que lo que se castiga es su participación en tales espectáculos. De esta forma dicha participación puede venir desarrollada en Internet mediante shows en directo que permiten su visionado desde cualquier parte del mundo, convirtiendo de ese modo la conducta en un ciberdelito.

[115] Como veíamos antes a esta conducta le puede preceder la del art.183.ter que incrimina la de quien a través de tecnologías de la información y la comunicación contacte con un menor de 16 años para que realice los comportamientos previstos en este art.189. No obstante los sujetos pasivos protegidos por el art.183 son los menores de 16 años, y en cambio el art.189 no incluye edad alguna lo cual lleva a pensar que solo pueden ponerse en relación ambos preceptos cuando la edad del menor o de la persona con discapacidad necesitada de especial protección no alcance los 16 años, ya que de hacerlo solo entraría en aplicación el último artículo.

[116] En este sentido puede darse la situación en que se capte a un menor para elaborar material pornográfico cuando ya sea mayor de edad, lo cual daría lugar a penalizar un comportamiento contrario a la finalidad que se pretende buscar con la norma.

Lo relevante es que el espectáculo en el que participe el menor sea calificado como exhibicionista o pornográfico. Para ello habrá que atender a los art.185 y 186 donde se describen estos actos. Además para calificar el acto como pornográfico habrá que estar a su conjunto y al específico papel que juegue el menor dentro de él.

- La segunda conducta castiga la **elaboración de material pornográfico**, su creación, habiendo intervenido menores o personas con discapacidad necesitadas de especial protección con el fin generalmente de que luego sea comercializado, (aunque eso ya entra dentro del siguiente apartado de este mismo número). Dicha creación puede producirse por medios informáticos al no haber limitado el precepto el modo en que deba elaborarse, de ser así el artículo se encuadra dentro de la ciberdelincuencia.

Del supuesto quedan excluidos como sujetos activos quienes asistan a tales espectáculos o posean el material elaborado por menores o personas con discapacidad necesitadas de especial protección, pues tales comportamientos ya quedan penados en los apartados cuarto y quinto del mismo artículo, que posteriormente serán objeto de estudio.

Los sujetos pasivos son los menores de 18 años pero mayores de 16, puesto que los menores de 16 años gozan de una protección reforzada en el número segundo del mismo artículo mediante una agravante.

Un aspecto importante en la elaboración de pornografía infantil es la posible relación concursal con los delitos contra la intimidad del art.197 cuando la víctima no sepa que está siendo filmada en una relación sexual que ha consentido mantener. Para ello se requeriría el dolo del autor, que actúe a sabiendas y con la intención de menoscabar su intimidad. Sin embargo se viene entendiendo que como el menor no es consciente de que está siendo grabado, su indemnidad sexual no queda vulnerada[117].

Finalmente, cuando los hechos descritos en esta primera letra del art.189 se realicen mediando violencia o intimidación, el tercer número del mismo artículo prevé una agravante.

"Si los hechos a que se refiere la letra a) del párrafo primero del apartado 1 se hubieran cometido con violencia o intimidación se impondrá la pena superior en grado a las previstas en los apartados anteriores".

A continuación en la letra b) del apartado primero de este mismo artículo se incluye la conducta de quien produce, distribuye, exhibe, ofrece o facilita la producción, venta,

[117] MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, p.119.

difusión o exhibición de pornografía en la que han intervenido menores o personas con discapacidad necesitadas de especial protección.

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

La conducta pertenece al mismo ámbito típico relativo a la instrumentalización de menores o personas con discapacidad necesitadas de especial protección para realizar comportamientos de índole sexual en el que se utilizan como objetos sexuales.

El comportamiento tiene lugar en un momento temporal posterior al de la letra anterior, puesto que se produce una vez que el material pornográfico ya ha sido elaborado y el autor procede a ponerle en circulación mediante las conductas que el tipo refleja, tales como la venta, difusión o exhibición.

> En este entorno de la pornografía infantil es donde la citada reforma de 2015 aporta una de sus principales novedades al introducir un **concepto de pornografía infantil**[118] o de material en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección.
>
> Con anterioridad a dicha reforma se planteaban problemas interpretativos en relación a este precepto y a otros cuyo objeto material es la pornografía infantil. Ahora la reforma introduce en el mismo art.189.1.b) cuatro definiciones de lo que se considera como tal, estos son:
>
> > a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada.
> >
> > b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales.
> >
> > c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser

[118] GARCÍA ÁLVAREZ P., "El menor como sujeto pasivo de delitos, con especial referencia a los delitos contra la libertad e indemnidad sexual y los cambios en ellos introducidos por el proyecto de Ley Orgánica de 20 de septiembre de 2013", *Revista General de Derecho Penal*, 2013, pp. 37-38.

un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.

d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales.

El concepto que se da de pornografía infantil es bastante extenso, llegando a comprender situaciones controvertidas.

Del precepto se desprende que lo que se protege es tanto la conducta sexual del menor o de la persona con discapacidad necesitada de especial protección como la representación de sus órganos sexuales. Además se utiliza el concepto "representación visual", por lo que la pornografía que pudiera expresarse en un soporte escrito o auditivo quedaría exenta de responsabilidad penal. Esto sería por ejemplo un relato de contenido sexual en el que sus personajes sean menores de edad.

Como consecuencia de ello, con la citada reforma se suprime la redacción del anterior art.189.7 dándole un contenido diferente. Antes de la reforma en ese número se castigaba a quien *produjera, vendiera, distribuyera, exhibiera o facilitara material pornográfico en el que no habiendo sido utilizados directamente menores o incapaces, se empleara su voz o imagen alterada o modificada*. Se trataba de "pseudo pornografía infantil", donde en realidad no llegaba a afectarse la indemnidad sexual de los menores al alterar solo la parte gráfica o auditiva, por ello la doctrina criticaba la vigencia del citado tipo al carecer de una base pornográfica real.

El motivo por el que se ha despenalizado el supuesto ha sido el concepto que se da de pornografía infantil en la reforma, que excluye la que se exprese en un soporte escrito, auditivo o virtual.

Respecto al resto del concepto de pornografía infantil, la letra c) incluye en la letra c) un aspecto polémico al considerar como tal la realizada por una persona mayor de edad pero aparentando ser menor. No parece guardar relación con el principio de proporcionalidad el que se castiguen situaciones en las que los actores siendo mayores de edad por aparentar un aspecto más infantil de lo que son en realidad sean penados. Sin embargo este apartado es de carácter *iuris tantum* y admite prueba en contrario al eximir de responsabilidad si se logra demostrar que en el momento de realizar el material pornográfico el sujeto alcanzaba la mayoría de edad.

Finalmente el término "imágenes realistas" al que alude la letra d) es difícil de entender, pues ya están aparentemente penadas en las letras anteriores. Se puede interpretar que se refiere a supuestos donde no son actores de verdad los que participan, sino que son imágenes creadas de manera virtual en las que se representa a menores.

El tipo no distingue grados de participación a la hora de realizar tales conductas por lo que se hace difícil poder diferenciar entre autores y cómplices en los supuestos de codelincuencia. De este modo el precepto abarca todo el proceso desde que se capta a alguien para realizar material hasta que este se elabora y finalmente se distribuye, castigando a todos los que intervienen en sus diferentes fases.

De todas las conductas por las que se consuma el delito, la mayoría se realizan generalmente en Internet al ser donde tienen más trascendencia debido a su rápida difusión en páginas web o redes sociales abiertas a millones de personas. Además Internet permite crear páginas específicas dedicadas a la distribución de pornografía infantil que almacenan gran cantidad de material haciendo del problema un fenómeno difícil de resolver por su rápida expansión a través del ciberespacio. En este sentido cuando la circulación a la que alude el precepto venga expresada por medio de tecnologías de la información y la comunicación estaremos ante una manifestación más de la ciberdelincuencia en nuestro ordenamiento.

Junto a ello el artículo no hace alusión específica a la forma de llevar a cabo tales comportamientos, sino que utiliza el genérico "por cualquier medio", incluyendo todos los comportamientos en la red.

Llama la atención el último inciso de esta letra al incluir dentro de las conductas típicas la de quien lo "poseyera para estos fines", por lo que no solo castiga el reparto en sí mismo de dicho material, sino además a quien lo tiene en un momento concreto y aún no lo ha puesto en circulación pero tiene la intención de hacerlo en un futuro.

A todo ello se añade que es irrelevante para el Derecho penal el origen del material, e incluso que se desconozca su autoría, pues se castiga también la circulación del mismo cuando ha sido realizado en el extranjero o fuere desconocido quien lo elaboró. Esto supone una excepción al principio de territorialidad, según el cual la ley penal se aplica a supuestos cometidos en España, ya que en el precepto de ser así se castigarían conductas acaecidas fuera del territorio nacional. Sin embargo lo que parece desprenderse del precepto es que lo que se castiga es la distribución en España cuando ha sido elaborado fuera de ella, es decir que a lo que se refiere es a la puesta en circulación (que deberá ser en España), y no a su origen que no determina la competencia de los tribunales españoles.

En el art.189.2 se prevén circunstancias **agravantes** comunes a las dos letras del primer número para cuando en las conductas anteriormente descritas concurran las siguientes circunstancias:

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

Algunas de estas agravantes ya estaban previstas en la anterior redacción, pero se incluyen las relativas al peligro en que se pone a la víctima, la importancia que genere dicho material y la reincidencia del autor, así como los cambios terminológicos de incapaz por personas con discapacidad necesitadas de especial protección y el aumento de la edad para realizar estos comportamientos a 16 años.

A continuación, el apartado cuarto del art.189 se modifica tras la reforma introducida por la LO 1/2015 introduciendo un supuesto atípico hasta el momento, el del particular que asista a espectáculos exhibicionistas o pornográficos sabiendo que participan menores o personas con discapacidad necesitadas de especial protección [119].

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

[119] Con la introducción de el nuevo apartado cuarto se sustituye al que hacía referencia en la anterior redacción al comportamiento de quien haga participar a un menor o incapaz en un comportamiento de naturaleza sexual que perjudique la evolución o desarrollo de su personalidad. Ello ahora se ha introducido en el art.183.bis como antes se estudió. El motivo del cambio fue que tal conducta no encajaba del todo en este ámbito de corrupción de menores al haber regulado ya los supuestos de prostitución, participación en espectáculos exhibicionistas o pornográficos, y los de abusos, agresiones, exhibicionismo o provocación sexual, además de lo indeterminado del precepto.

La conducta es dolosa, siendo necesario que el autor sepa que quien participa en dichas actuaciones es menor o es una persona con discapacidad necesitada de especial protección, puesto que de no saberlo y actuar con error la conducta sería impune al no estar prevista su comisión culposa.

La reforma en su intento por acabar con la corrupción de menores en todos los ámbitos incluye otro supuesto en el quinto apartado que afecta a los particulares y que da lugar a otro delito informático al mencionar incluso expresamente a las tecnologías de la información y la comunicación. Se trata de castigar la **posesión y adquisición para uso privado de pornografía infantil** en los términos descritos por el apartado primero. La conducta debe ser dolosa pues el autor debe adquirirla sabiendo la minoría de edad o discapacidad de las personas que participan en ella.

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

Este comportamiento ya estaba previsto con anterioridad a la reforma de 2015 en el apartado segundo del art.189, donde lo que se castiga en realidad son actos preparatorios de una ulterior conducta relacionada con la distribución que es lo que verdaderamente atenta contra la indemnidad sexual del menor al tener una repercusión mayor. Sin embargo el hecho se castiga en sí mismo al consumarse el delito con la mera posesión para uso propio, sin que sea necesario tener relación con quien lo elaboró o participar en tal proceso.

Con la reforma de 2015 se incluye un nuevo supuesto en el segundo párrafo del número quinto para quien acceda de forma puntual aunque intencional a pornografía infantil por cualquier medio, mencionándose expresamente las tecnologías de la información y la comunicación, como Internet por ejemplo.

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

Con esta nueva previsión sería delito por ejemplo acceder de forma esporádica a una página en Internet donde se muestre este contenido, aunque debiendo concurrir el ánimo de encontrar material de carácter pornográfico infantil.

> No obstante algún sector de la doctrina como el catedrático MUÑOZ CONDE es contrario a este tipo penal pues considera que el Derecho penal no puede intervenir en la

> intimidad del individuo para tipificar una conducta que por muy inmoral que parezca no vulnera la indemnidad sexual del menor o persona con discapacidad necesitada de especial protección de manera directa. Para proteger a los sujetos pasivos ya existen delitos que castigan a quienes elaboran y difunden el material, pero de ahí a tipificar a quien lo posea de manera privada no parece razonable ni coherente con el principio de intervención mínima del Derecho penal o con el derecho constitucional a la intimidad.
>
> Además compara esta conducta con el consumo y posesión de drogas, que es atípica hasta cierta cantidad castigando solo el tráfico, ya que aunque el consumo favorezca dichas conductas la mera posesión no debe ser castigada al existir otros mecanismos en el ordenamiento jurídico menos restrictivos de derechos y que proporcionan solución al problema. Igual respuesta debería darse a juicio de dicho autor con la posesión de pornografía infantil.

El artículo se cierra con una serie de disposiciones comunes a todos los comportamientos relativos a la corrupción de menores y pornografía infantil.

En primer lugar el número sexto castiga a las personas responsables de los menores o personas con discapacidad necesitadas de especial protección, es decir sus padres, tutores, guardadores o curadores, cuando sabiendo que son objeto de las prácticas descritas en este capítulo no hagan lo posible para impedirlo.

> *"El que tuviere bajo su potestad, tutela, guarda o acogimiento a un menor de edad o una persona con discapacidad necesitada de especial protección y que, con conocimiento de su estado de prostitución o corrupción, no haga lo posible para impedir su continuación en tal estado, o no acuda a la autoridad competente para el mismo fin si carece de medios para la custodia del menor o persona con discapacidad necesitada de especial protección, será castigado con la pena de prisión de tres a seis meses o multa de seis a doce meses."*

Se trata de un supuesto de comisión por omisión en el que es preciso que los sujetos activos conozcan de la situación en que se encuentra el menor y no hicieran nada para evitarlo, ya sea por ellos mismos o acudiendo a la autoridad.

En el número siguiente, el séptimo, se permite al Ministerio Fiscal que prive de la patria potestad, tutela, guarda o acogimiento a los autores de la conducta del anterior artículo, es decir quienes no impedían que menores o personas con discapacidad necesitadas de especial protección siguieran siendo objeto de explotación sexual.

> *"El Ministerio Fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior".*

Finalmente el artículo se cierra con una reforma más en el ámbito de la ciberdelincuencia tras la reforma de 2015, y que permite a los jueces cerrar las páginas web que muestren pornografía infantil, así como bloquear su acceso a ciertos usuarios.

> *"Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de Internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español".*

La inclusión de este último precepto es un paso más en la lucha contra la pornografía infantil, ya que el principal vehículo por el que se propaga es la red donde es relativamente sencillo encontrar tales páginas con contenido ilícito.

Con la nueva previsión que incluye el octavo apartado del art.189 se podrá ir disminuyendo tal lacra en la red a pesar de lo difícil que es controlarla, pues la facilidad y rapidez con la que se crean nuevas páginas es mayor a la que avanza la justicia. No obstante cerrar las páginas provocará que quienes se lucran a costa de menores y personas con discapacidad necesitadas de especial protección dejen de recibir gran parte de sus ingresos, además de evitar que posibles pedófilos accedan a tales contenidos generando futuras conductas delictivas.

3.3 Delitos de difusión de material pornográfico y provocación sexual en la red de menores o personas con discapacidad necesitadas de especial protección. Relevancia penal de las webs pornográficas

El Capítulo III del Título VIII de su Libro II del Código Penal en los arts.185 y 186 regula los delitos de exhibicionismo y provocación sexual. Estos delitos forman la última de las conductas que atentan contra la libertad sexual en materia de delincuencia informática.

Al igual que sucedía en las conductas anteriores se trata de dos delitos en los que solo los menores o personas con discapacidad necesitadas de especial protección pueden ser los sujetos pasivos, pues la misma conducta no será constitutiva de delito cuando se lleve a cabo ante adultos.

Ambos preceptos no han sido objeto de modificación en la reforma del Código Penal introducida por la LO 1/2015 por lo que la versión que conservamos de ellos se mantiene desde 1999 con la misma redacción.

Son dos delitos con los que se protege al menor o a la persona con discapacidad necesitada de especial protección cuando se ve involucrado en actos de naturaleza sexual que pueden incidir negativamente en su indemnidad sexual o excitarle indebidamente[120].

La terminología de tales preceptos es bastante abstracta al utilizar términos como "obsceno" o "pornográfico", lo que dificulta enormemente su interpretación al depender de la moralidad sexual de la sociedad de cada época.

Ambas conductas pueden ser susceptibles de constituir un delito informático al poder ser realizadas mediante el uso de tecnologías de la información y la comunicación, Sin embargo en el delito del art.186 se aprecia con mayor claridad la estrechez que mantiene con la ciberdelincuencia.

En primer lugar el delito de **exhibicionismo** se contempla en el art.185 en los siguientes términos:

> *"El que ejecutare o hiciere ejecutar a otra persona actos de exhibición obscena ante menores de edad o incapaces, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses".*

Se trata de una conducta por la que el autor exhibe sus órganos sexuales genitales (u otras partes de su anatomía que puedan dar lugar al mismo fin y afectar de igual modo a la indemnidad sexual a un menor o persona con discapacidad necesitada de especial protección), con el fin de excitarse sin que sea necesario que tenga que haber relaciones sexuales entre ambos.

El aspecto relevante del tipo es el carácter de obsceno que deben revestir los actos del autor. Dicho carácter se aplica también al siguiente artículo relativo a la difusión de pornografía entre menores, lo que implica realizar una interpretación conjunta de ambos preceptos.

El elemento de obscenidad genera bastante indeterminación siendo vago e impreciso al depender en cierta medida del concepto moral que le otorgue la sociedad en cada época concreta, por lo que para su interpretación habrá que acudir a las pautas sociales.

[120] MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, p. 248.

Finalmente, la conducta requiere que el autor actúe de forma dolosa con la intención de involucrar a la víctima con su acción en un contexto sexual, debe tener el carácter erótico necesario para producir la lesión en la indemnidad sexual del menor o de la persona con discapacidad necesitada de especial protección. Por tanto no cabe cometer el delito de forma imprudente, por lo que en los casos en que el autor desconozca la edad de la víctima pensando que era mayor de edad, el error al ser invencible quedaría impune.

La relación del citado tipo penal con la ciberdelincuencia es estrecha, pues en ningún momento se desprende del tipo ni de su finalidad que tenga que haber una presencia física de los sujetos en el momento de realizarse la conducta[121], de ahí que pueda ser llevada a cabo a cabo mediante un medio telemático con el que sea posible realizar actos de exhibición obscenos en los mismos términos que el precepto señala. Por ejemplo podría suceder mediante el chat de una red social o con aplicación para móviles Whatsapp, que permite enviar imágenes o videos.

En segundo lugar encontramos en el art.186 el delito de **difusión de material pornográfico** que se encuentra regulado de la siguiente manera:

> *"El que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre menores de edad o incapaces, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses".*

La conducta que castiga el precepto es la venta, difusión o exhibición de material pornográfico[122] a menores o personas con discapacidad necesitadas de especial protección, quedando exentas de responsabilidad penal las mismas conductas dirigidas hacia a mayores de edad. Todas ellas se caracterizan por su alto contenido pornográfico donde el menor entra en contacto con él de forma directa tras la acción del autor.

---

[121] Según esta opinión MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, p.107.

[122] La alusión al material pornográfico genera problemas interpretativos al igual que antes lo hacía el término obsceno. La reforma de este año clarifica la situación en relación a la pornografía infantil como antes se explicó al detallar lo que se considera como tal, pero no da un concepto a nivel general con el que se explique que se considera material pornográfico. Por esta razón se generan dudas en función de si dicho material debe venir expresado de forma audiovisual o si por el contrario podría estar plasmado de manera escrita mediante un relato por ejemplo. Además se duda si en el concepto de material pornográfico se incluye la denominada pornografía "blanda" o no, entendiendo por esta la que no comprende actos sexuales que incluyan violencia, menores o animales por ejemplo que quedan reconducidos a la categoría de pornografía "dura". En opinión de MUÑOZ CONDE todo material pornográfico debe servir para provocar sexualmente a quien lo observa, siendo indiferente el soporte por el que venga expresado, ya sea escrito, hablado o gráfico, como el cine o el video.

La conducta típica se produce en un momento posterior a la elaboración de dicho material, cuando ha sido puesto en circulación y entra en contacto con los destinatarios finales. Por ello las conductas anteriores son atípicas en este ámbito.

La razón por la que tales conductas son punibles es debido a que se considera que el visionado de material pornográfico es susceptible de producir daños en el desarrollo de la personalidad de personas inmaduras o con discapacidad necesitadas de especial protección. De este modo el legislador no solo castiga la realización física de conductas sexuales sino también su observación.

Además, lo que incrimina el artículo son las conductas que hacen posible la aproximación al menor del material pornográfico no en las que el menor participe en los actos o espectáculos, pues eso ya se tipifica en el art.189. Por ello precepto queda reducido al mero visionado de menores o personas con discapacidad necesitadas de especial protección de material pornográfico, castigando a quien se lo facilita.

En este sentido el precepto es claro al exigir un **medio directo** por el que menor entre en contacto con el material pornográfico, por lo que quedan excluidas de relevancia penal las situaciones donde el material se dirige a una pluralidad indeterminada de personas y no a alguien concreto, por ejemplo el caso de las páginas web pornográficas o de las revistas pornográficas que se exhiben en un kiosco. De este modo el medio por el que se desarrolla la conducta no es libre, requiriendo un contacto directo entre el menor o la persona con discapacidad necesitada de especial protección y la fuente de la que emana el material pornográfico. Esta situación se dará tanto en el mundo real adquiriendo una revista por ejemplo, como en el virtual en el transcurso de una conversación online, (produciéndose el ciberdelito).

Por ello la variedad de formas de comisión es amplísima, no solo en el mundo virtual sino también en el real.

> Sin embargo dentro del mundo virtual se plantea un problema con las **páginas web que contienen material pornográfico** debido a que el artículo requiere que el delito se produzca a través de un *medio directo* entre autor y víctima y que el autor actúe con el dolo de involucrar al menor o persona con discapacidad necesitada de especial protección en un entorno sexual. Ello genera problemas de aplicación cuando el menor visita tales páginas entrando en contacto con el material. El problema no es baladí desde el momento en que en Internet hay millones de páginas web con contenido sexual que van dirigidas a cualquier

usuario en general y en las que es verdaderamente fácil y sencillo el acceso por parte de cualquiera sin apenas controles acerca de su edad.

En este sentido un sector de la doctrina como TAMARIT SUMALLA[123] se opone a que el tipo pueda consumarse cuando el menor accede a dicho material en Internet puesto que lo que busca penar el art.186 es la confrontación directa de la víctima con la pornografía, no pudiendo castigarse cualquier tipo de acción realizada con objetos pornográficos a través de Internet.

En el Derecho español la difusión de material pornográfico no es constitutiva de delito, ya que solo cuando se dirige a menores o personas con discapacidad necesitadas de especial protección lo es. Los actos que deben ser penados en el ámbito de la difusión de pornografía son los que atentan contra la libertad sexual en sentido estricto, es decir únicamente cuando producen una confrontación directa entre la víctima y la pornografía. De ahí que no tenga que ser castigada cualquier conducta que se produzca a través de Internet con material pornográfico aunque intervengan menores o personas con discapacidad necesitadas de especial protección, pues lo que hay que ver es si el ánimo de tal acción fue el de involucrar a la víctima en el ámbito sexual.

La solución por tanto pasa por la determinación del elemento subjetivo, pues durante toda la conducta debe concurrir el dolo directo del autor tendente a involucrar al menor concreto en un entorno sexual.

De ello se extraen las dos principales conclusiones, la primera y como apuntábamos antes es que se requiere que el autor y la víctima se relacionen por un medio directo, lo cual en páginas web de Internet no sucede, (si bien en otros entornos de Internet como los chats de las redes sociales si, por lo que no cabe la exclusión de este tipo penal en el marco de Internet y por ende la ciberdelincuencia); y en segundo lugar, que cabría llevar a cabo la conducta mediante dolo eventual, ello dependerá de que el autor cuando distribuya el material pornográfico en la red sea consciente o no del posible alcance a dicho material de menores o personas con discapacidad necesitadas de especial protección y haga lo posible por evitarlo desplegando una diligencia adecuada para ello, ya que de no ser así cuando el menor entre en contacto con el material en lugar de apreciarse error vencible por parte del autor (que daría lugar a la impunidad), se aplicaría el dolo eventual haciendo que se consume el tipo penal.

El delito se consuma cuando el material queda a disposición del menor o de la persona con discapacidad necesitada de especial protección, por lo que cuando dicho material sea elaborado pero no llegue a entrar en contacto de manera directa con las

[123] véase TAMARIT SUMALLA, J. M., *La protección penal del menor frente al abuso y explotación sexual*, Aranzadi, Navarra, 2000, p.139-141.

víctimas la conducta quedará exenta de responsabilidad penal. Esta idea es consecuencia de la licitud de la pornografía en Internet, así como de su comercio.

Por ello solo cuando expresamente se dirige hacia menores o personas con discapacidad necesitadas de especial protección estaremos ante este tipo penal, haciendo que el hecho de que haya páginas webs pornográficas no tenga relevancia penal en cuanto a su difusión hacia menores al dirigirse a un público indeterminado. Dependerá de la intención del creador de la página y de la seguridad con que proteja a la misma frente a los accesos de quienes no tienen edad o madurez para visitarla.

De este modo el delito en Internet queda reducido al ámbito en que autor y víctima mantienen un contacto directo entre sí y el primero le hace entrar en contacto con el material pornográfico, ya sea mediante su venta, difusión o exhibición.

Como señalábamos antes, el aspecto subjetivo del tipo queda revestido por un especial injusto mediante el ánimo lascivo o la intención de involucrar al menor en un contexto sexual haciéndole llegar dicho material. Por ello se requiere en todo momento la concurrencia del dolo del autor. En este sentido cabe traer a colación lo apuntado más arriba acerca del dolo del autor con el que debe provocar sexualmente al menor, lo que a juicio de parte de la doctrina no sucede cuando la difusión se produce hacia una pluralidad indeterminada de sujetos careciendo de relevancia penal, con la salvedad del posible dolo eventual en que podría incurrir.

Al igual que sucedía en el delito de exhibicionismo, cuando el material llegue al menor de manera culposa, ya sea por error invencible del autor o por casualidad, el delito quedaría impune al no estar prevista su comisión culposa. En este mismo sentido cuando el material llegue el menor por motivos educativos por ejemplo, la conducta también quedaría exenta de responsabilidad al no concurrir el ánimo de provocarle sexualmente.

Para concluir el estudio del artículo cabe indicar que el hecho de que en la citada reforma no se haya modificado genera problemas de congruencia con el resto del Título, pues se permite a un mayor de 16 de años, (13 en la anterior redacción) consentir mantener relaciones sexuales, e incluso por debajo de esa cifra cuando medie el consentimiento libre, pero no comprar material pornográfico hasta que no alcance la mayoría de edad.

De este modo, en un ámbito de mayor trascendencia para la indemnidad sexual del menor como es el de mantener relaciones sexuales se posibilita que pueda consentir, pero en otro como es el acceso a material pornográfico se le protege durante toda su minoría de edad con independencia de su voluntad[124].

[124] Según esta opinión GARCÍA ÁLVAREZ, P., "El menor como sujeto pasivo de delitos, con especial referencia a los delitos contra la libertad e indemnidad sexual y los cambios en ellos introducidos por el proyecto de Ley Orgánica de 20 de septiembre de 2013", *Revista General de Derecho Penal*, 2013, pp. 30-31.

SECCIÓN SEXTA: **DELITOS DE INJURIAS Y CALUMNIAS**

1. Introducción

Los delitos contra el honor presentan cierta especificidad penal y sobre todo procesal ya que son los únicos delitos privados que aparecen en el Código, por lo que requieren unas condiciones especiales para llevar a cabo su persecución, tales como la previa querella por el ofendido. Además el Ministerio Fiscal no participa en el proceso.

En estos delitos el honor como bien jurídico protegido es muy difícil de observar penalmente al ser muy relativo. Ello implica que lo que para alguien puede suponer una vulneración de su honor, para otro no lo sea.

Para conseguir determinarlo el Derecho penal lo que hace es apreciarlo por un lado de forma objetiva, es decir atendiendo a las cualidades externas que tiene una persona, y por otro subjetivamente, mediante la propia estimación de una persona hacia sí mismo[125].

Los tipos penales que protegen el honor contemplan acciones destinadas a menoscabar la fama o estimación de otra persona. Cuando el cauce por el que se realicen tales acciones sea una nueva tecnología o artificios similares estaremos ante un delito informático.

De este modo adquieren relevancia penal las expresiones que se vierten en portales de Internet como redes sociales o páginas de opinión y en las que se menoscaba la fama o estimación de otra persona. Además, estos medios permiten que su ejecución sea muy sencilla y otorgan a los autores un anonimato mayor que cuando son manifestadas fuera de un soporte informático.

> Ejemplos[126] de ello encontramos en Sentencias como la de la Audiencia Provincial de Toledo de 8 de enero de 2014 en relación a un grupo de menores que vertieron expresiones difamatorias en redes sociales como Facebook a unos compañeros de su clase. O la

[125] MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, pp. 296-298.

[126] MENDO ESTRELLA, A., "Delitos y Redes Sociales: mecanismos formalizados de lucha y delitos más habituales. El caso de la suplantación de identidad", *Revista General de Derecho Penal,* 2014*,* pp.27-28.

> Sentencia de la Audiencia Provincial de Castellón el 27 de noviembre de 2012 cuando el autor valiéndose de la misma red social profirió estas expresiones contra una Policía Municipal después de que esta retirara su vehículo debido a su mal estacionamiento.
>
> En otros casos se va más allá como recoge la Sentencia del Juzgado de lo Penal nº 4 de Segovia, donde además de realizar acciones similares a las anteriores, el perfil que utilizaron en dichas redes era falso haciéndose pasar por otra persona.

Por la naturaleza del delito y por las exigencias relativas a que sea cometido por medio de un soporte informático para que sea calificado como ciberdelito, los supuestos en los que aparecen quedan bastante reducidos en la práctica a casos donde las expresiones que atentan contra la fama o la propia estimación de la persona son vertidas en redes sociales.

2. Regulación penal

Su regulación se encuentra en el Título XI del segundo Libro del Código Penal[127]. No obstante hay que tener en cuenta otros preceptos dirigidos a proteger el honor de ciertas personas como el del Rey o de las Cortes Generales.

> Junto a esta protección penal se encuentra otra de carácter civil reconocida en la Ley Orgánica 1/1982. La elección queda en manos del particular dada la especial naturaleza del delito, por lo que será la víctima quien podrá elegir si a la vía civil en lugar de interponer la obligatoria querella para iniciar la acción penal.

En la regulación penal contenida en los artículos 205 y ss. se establecen dos delitos específicos, por un lado el de injurias y por otro el de calumnias.

2.1 Injurias

El tipo básico se regula en el art.208 que establece:

> *"Es injuria la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación".*

Se castigan las acciones o expresiones dirigidas a lesionar el honor de otra persona, entendido este como la fama o la propia estimación. Es decir que el delito se comete cuando se vulnera alguno de los dos contenidos del honor, ya sea la fama o la propia estimación, (dimensión externa e interna del mismo respectivamente).

[127] http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t11.html

> Dentro de las injurias se distinguen dos categorías, las injurias reales y las irreales.
>
> En las denominadas injurias reales, el autor manifiesta expresiones o realiza comportamientos que van más allá de meras opiniones o juicios de valor, ya que se sustentan en hechos que permiten llevarlas a cabo, como por ejemplo difundir públicamente los defectos físicos de una persona. Estas injurias pueden ser cometidas mediante un comportamiento activo, como en el ejemplo anterior, o pasivo mediante una omisión, negando el saludo a otra persona por ejemplo.
>
> Junto a ellas encontramos las injurias irreales, que son acciones o expresiones que contienen juicios de valor o juicios de hecho.
>
> Ambos tipos de injurias pueden venir expresadas de forma escrita o verbal, puesto que el soporte por el que se desarrolla tal conducta delictiva es indiferente para su consumación siempre que se produzca la lesión en el honor del ofendido.

La lesión al honor debe ser grave, pero dicha gravedad debe ser entendida tal y como la sociedad lo concibe en el momento en que se produce el delito.

> *"Solamente serán constitutivas de delito las injurias que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto público por graves, sin perjuicio de lo dispuesto en el apartado 4 del artículo 173".*

Con esta previsión se posibilita que la acción penal no quede al arbitrio del ofendido, puesto que dependerá de un concepto social (atendidas la naturaleza, efectos y circunstancias del hecho) valorar si la expresión atenta contra el honor de esa persona o no.

Sin embargo la última reforma del Código Penal introducida por la LO 1/2015 ha añadido un último inciso a este párrafo en forma de excepción, pues cuando la injuria se refiere a las personas del art.173.2[128] bastará con que sea leve en lugar de grave como viene siendo exigido con carácter general para que sea constitutiva de delito.

Además la acción debe ser dolosa y en ningún caso cabe la culpa. En este sentido el artículo exige que para que el delito se produzca las expresiones manifestadas sean graves, para lo que el autor deberá actuar sabiendo su falsedad, (dolo directo), o teniendo un

[128] Tales personas son quien sea o haya sido cónyuge del autor; o sobre persona que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia; o sobre los descendientes, ascendientes o hermanos por naturaleza, adopción o afinidad, propios o del cónyuge o conviviente; o sobre los menores o personas con discapacidad necesitadas de especial protección que con él convivan o que se hallen sujetos a la potestad, tutela, curatela, acogimiento o guarda de hecho del cónyuge o conviviente; o sobre persona amparada en cualquier otra relación por la que se encuentre integrada en el núcleo de su convivencia familiar; así como sobre las personas que por su especial vulnerabilidad se encuentran sometidas a custodia o guarda en centros públicos o privados.

temerario desprecio hacia la verdad, (dolo eventual), por lo que se excluye la culpa dentro del tipo subjetivo de las injurias.

> *"Las injurias que consistan en la imputación de hechos no se considerarán graves, salvo cuando se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad".*

Por tanto las expresiones que hayan sido llevadas a cabo sin saber que eran falsas o sin un temerario desprecio hacia la verdad, aunque objetivamente pudieran serlo quedan fuera del tipo penal.

El delito se consuma en el momento que llega al conocimiento del ofendido, por lo que cabría su comisión en grado de tentativa si no llega por causas ajenas a la voluntad del autor. No obstante al ser un delito únicamente perseguible a instancia de parte difícilmente se podra iniciar la acción si no ha llegado a su conocimiento.

Se contempla una pena superior para cuando la injuria lleve aparejada publicidad. Esta agravante en el caso de los delitos informáticos casi siempre será de aplicación ya que para estar ante uno de ellos es necesario que la acción sea realizada mediante un soporte informático, y por su propia esencia estos tienden a difundirse públicamente.

> *"Las injurias graves hechas con publicidad se castigarán con la pena de multa de seis a catorce meses y, en otro caso, con la de tres a siete meses".*

De este modo la pena depende de que concurra esa circunstancia.

Finalmente, cabe la posibilidad como indica el art.210 de quedar libre de responsabilidad si los hechos que se manifiestan son ciertos y son referidos contra funcionarios públicos sobre hechos concernientes al ejercicio de sus cargos o referidos a la comisión de faltas penales o de infracciones administrativas.

> *"El acusado de injuria quedará exento de responsabilidad probando la verdad de las imputaciones cuando éstas se dirijan contra funcionarios públicos sobre hechos concernientes al ejercicio de sus cargos o referidos a la comisión de infracciones administrativas".*

Es la denominada *exceptio veritatis,* por la que queda fuera de responsabilidad penal lo que en principio pueda parecer injurioso pero posteriormente resulta ser cierto. Sin embargo dicha excepción queda reducida a los supuestos en que las injurias se han manifestado contra funcionarios sobre hechos concernientes al ejercicio de sus cargos o referidos a la comisión de faltas penales o de infracciones administrativas.

2.2 Calumnias

Como señala el art.205 son calumnias la expresiones consistes en la imputación de un delito. A diferencia del caso anterior en el que se castigaban las opiniones o juicios de valor que menoscabaran el honor de las persona, ahora queda reducido a la imputación de un delito. Esto limita la subjetividad y hace más fácil su apreciación.

> *"Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad".*

En el caso de los delitos informáticos la imputación del delito deberá venir expresada en un soporte informático como una red social por ejemplo.

Se trata de la imputación de un delito y no de una falta, cualquiera que sea el tipo penal. Además, es indiferente el grado de ejecución y de participación, y el delito que se manifiesta debe ser falso, ya que de no serlo quedaría exento de responsabilidad penal.

Se deben imputar hechos concretos que recaigan sobre alguien determinado. Y al igual que en el caso anterior si la calumnia se realiza mediante publicidad se impondrá una pena mayor.

El delito requiere siempre el dolo, ya sea directo o eventual. Se consumará en el momento que llegue a conocimiento de la víctima, quedando cometido en grado de tentativa de no hacerlo.

A diferencia de las injurias donde para excluir la responsabilidad penal se requería que las imputaciones se hubieran dirigido contra funcionarios públicos (se trataba de una excepción), ahora en las calumnias si se demuestra que el hecho delictivo que se atribuye a la otra persona es cierto el autor quedaría libre de responsabilidad en cualquier caso como indica el art.207.

> *"El acusado por delito de calumnia quedará exento de toda pena probando el hecho criminal que hubiere imputado".*

Finalmente, las disposiciones comunes a estos Títulos tienen especial relevancia para el supuesto de los delitos informáticos.

Del art.211 se extrae que las conductas llevadas a cabo mediante soportes informáticos se considera que se han realizado con publicidad, siendo estos el medio idóneo para hacer de este delito un ciberdelito.

> *"La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante".*

Dichos soportes quedan incluidos en la cláusula abierta de *cualquier otro medio de eficacia semejante,* que permite incluir todo lo manifestado por medio de Internet y por soportes informáticos que faciliten su difusión masiva.

Además en estos casos, como indica el art.211, respondería de forma civilmente solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

SECCIÓN SÉPTIMA: **DELITOS DE AMENAZAS Y COACCIONES**

1. Introducción

Las amenazas y las coacciones son dos delitos que atentan contra la libertad de las personas al impedir la libre formación de la voluntad de la víctima en un sentido amplio. En ellos la voluntad de la víctima queda doblegada a merced del autor.

Las amenazas y coacciones no van a suponer una restricción a la circulación en sentido estricto de la víctima, sino que mediante la exteriorización por parte del autor de ciertos comportamientos se va a infundir un temor en ella que limitará su capacidad de decisión.

Cuando el modo en que el autor manifieste su propósito sea un soporte informático o un artificio técnico estaremos ante un delito informático de amenazas o coacciones.

Al igual que sucedía en el caso de las injurias o calumnias, las nuevas tecnologías de la información y la comunicación han facilitado la comisión de estos delitos al ser más fácil ponerse en contacto con la víctima y realizar el comportamiento ilícito.

En el caso de las amenazas la conducta consistirá en el anuncio de un mal relacionado con la comisión de un delito en la persona de la víctima o en la de un tercero cercano a ella, al que le podrá acompañar o no una condición que evitaría que el mal se produjera; y en el de las coacciones en obligar a la víctima a hacer algo que no quiere o impedirle hacer lo que desea.

> Hay abundantes ejemplos en la jurisprudencia, por ejemplo la Sentencia de la Audiencia Provincial de Las Palmas de 11 de junio de 2013 recoge un supuesto de amenazas no condicionales en el que una persona empezó a publicar mensajes en Facebook contra el administrador de su comunidad amenazándole de muerte.
>
> En relación al delito de amenazas condicionales hay sentencias como la de la Audiencia Provincial de Cádiz el 18 de mayo de 2012 donde una persona tras haber roto con su pareja, por medio de Facebook la obligaba a retomar la relación, pues de lo contrario publicaría fotos íntimas obtenidas mientras estuvieron juntos.

En ambos casos la proliferación de las redes sociales y demás instrumentos informáticos constituyen el soporte material de dichos delitos. Tales medios a la vez garantizan una difusión mayor y aumenta las facilidades para su perpetración.

De ahí que para estar ante un delito informático será imprescindible el uso de estos artificios como cauce para cometer el tipo.

Además, en dichos delitos es frecuente el concurso de delitos que se produce, ya que aunque las amenazas o las coacciones se consuman en sí mismas, después pueden cometerse otros delitos como el de homicidio en el primer ejemplo u otro contra la intimidad en el segundo.

2. Bien jurídico protegido

Los delitos que se castigan en el Título VI están orientados a la protección de la libertad de la persona como bien jurídico protegido.

En los artículos ahí comprendidos se entiende la libertad en un sentido amplio, como libertad de actuación, es decir la capacidad de una persona para decidir lo que quiere o no quiere hacer, así como para trasladarse de un lugar a otro o situarse por sí misma en el espacio sin que su decisión se vea constreñida o mediatizada por otras personas[129].

De este modo la libertad se concibe como algo que deriva de la convivencia y de los propios condicionamientos que se imponen a la actuación del ser humano, lo que provoca que se configure como uno de los bienes jurídicos mas relativos que existen ya que entre otras cosas, la propia organización de un Estado supone en muchos ámbitos restricciones a la libertad de la persona, puesto que cada individuo no es libre del todo para comportarse como desee en ciertos contextos sociales o políticos.

Dentro de los tipos penales que nos ocupan en el ámbito de la ciberdelincuencia en materia de delitos contra la libertad, lo que se persigue es que el individuo pueda formar su libertad de forma voluntaria sin intromisiones ajenas.

3. Regulación penal

Se regulan en el Título VI del Código Penal[130] en los artículos 169 y siguientes.

[129] MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, p.152.
[130] http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t6.html

3.1 Amenazas

En el segundo Capítulo de este Título se tipifican las amenazas, entendidas como actos o palabras con las que infunde un temor racional y fundado relativo a la comisión de uno de los concretos delitos que el tipo penal estipula.

Mediante la acción se exterioriza el propósito de causar en la víctima un delito de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico (art.169).

> *"El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico (…)".*

La víctima puede ser tanto el propio amenazado, como su familia, u otras personas con las que estuviere vinculado.

Además es posible realizar una amenaza con un fin que no constituya delito (art.171), esta sería tal y como MUÑOZ CONDE[131] define, *la exteriorización hecha por una persona a otra del propósito de causarle a él, a su familia o persona allegada un mal, dependiendo luego del respectivo tipo delictivo la determinación de la naturaleza de dicho mal.*

> *"Las amenazas de un mal que no constituya delito serán castigadas con pena de prisión de tres meses a un año o multa de seis a 24 meses, atendidas la gravedad y circunstancia del hecho, cuando la amenaza fuere condicional y la condición no consistiere en una conducta debida. Si el culpable hubiere conseguido su propósito se le impondrá la pena en su mitad superior".*

El delito debe venir precedido de una acción por la que se exterioriza el propósito, que será un mal, ya sea un delito o no, y que se producirá en un futuro más o menos cercano.

El mal será real, serio y persistente aunque basta con una apariencia del mismo para su consumación, que deberá llegar a conocimiento del amenazado.

Además el mal debe ser grave y objetivamente debe servir para intimidar al amenazado, es decir estar fundado y que de modo racional proceda su credibilidad. Finalmente deberá recaer en la persona del amenazado, así como su familia o allegados.

[131] MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, p.159.

Junto a toda la acción es necesario que el autor actúe dolosamente y que tenga la intención de cometer el propósito si las amenazas fueran de carácter condicional.

Finalmente el delito se consuma en el momento en que llega al conocimiento del amenazado el propósito de causarle un perjuicio. De no ser así y no llegar a su conocimiento el delito quedaría cometido en grado de tentativa, aunque difícilmente se podrá perseguir al ser un delito semiprivado que requiere la previa denuncia por parte de la víctima, por lo que si no llega a conocer de él no podrá iniciar la acción penal.

Dentro de las amenazas el Código regula dos clases concretas:

3.1.1 Amenazas de un mal que constituye un delito

En esta categoría la regulación distingue entre:

A. Amenazas condicionales

En las amenazas condicionales el autor exige al amenazado que realice algo a cambio de no cometer el delito. La condición que el autor exige puede ser lícita o ilícita pero el mal tendrá que ser necesariamente un delito de los que el propio artículo incluye.

Y la pena varía en función del modo en el que se realice la acción y del resultado obtenido.

> *"Con la pena de prisión de uno a cinco años, si se hubiere hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito. De no conseguirlo, se impondrá la pena de prisión de seis meses a tres años".*

Este supuesto de amenazas condicionales comprende el delito específico de amenazas en el ámbito de la ciberdelincuencia, ya que tal conducta es agravada cuando se haya llevado a cabo por medio de un artificio técnico como un medio de comunicación o reproducción.

> *"Las penas señaladas en el párrafo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por* ***teléfono o por cualquier medio de comunicación o de reproducción,*** *o en nombre de entidades o grupos reales o supuestos".*

El precepto se encuadra dentro del ámbito de la ciberdelincuencia para los casos en que dichas amenazas se llevan a cabo por medio de un soporte informático.

Como se puso de relieve en los ejemplos planteados más arriba, las amenazas que se realizan por estos cauces son frecuentes al aportar mayores facilidades en su comisión. Además con el desarrollo de Internet se está aproximando su comisión a multitud de usuarios que ven en él una herramienta sencilla y eficaz para llevar a cabo tales acciones, haciendo que en los últimos años esta forma delictiva esté viéndose incrementada.

B. Amenazas no condicionales

La regulación se contiene en el mismo artículo y la acción es idéntica, difiriendo de la anterior amenaza en que el autor no introduce una condición a cambio de no producir el perjuicio en la víctima, sino que simplemente infunde el mal sin dar a la víctima ninguna "opción" para evitarlo.

> *"Con la pena de prisión de seis meses a dos años, cuando la amenaza no haya sido condicional".*

C. Amenazas con finalidad terrorista

Finalmente en el art.170 se incluyen las amenazas constitutivas de delito pero con finalidad terrorista cuando tengan como propósito atemorizar a grupos étnicos, culturales, religiosos…

3.1.2 Amenazas de un mal que no constituye un delito

Se encuentran reguladas en el art.171 en el que se detallan sus dos modalidades.

A. Amenazas condicionales

Se trata de un tipo de amenazas con idéntica estructura a las anteriores pero su objeto no es la comisión de un delito, o por lo menos no es uno de los delitos integrados en la lista que menciona el art.169.

> *"Las amenazas de un mal que no constituya delito serán castigadas con pena de prisión de tres meses a un año o multa de seis a 24 meses, atendidas la gravedad y circunstancia del hecho, cuando la amenaza fuere condicional y la condición no consistiere en una conducta debida. Si el culpable hubiere conseguido su propósito se le impondrá la pena en su mitad superior".*

El mal con el que se amenaza puede tanto lícito o ilícito, pero lo relevante para calificar este delito es la relación entre el mal con el que se amenaza y la pretensión que se pide.

B. Chantaje

Se regula el chantaje donde el autor impone una condición generalmente dineraria a cambio de no revelar hechos relativos a la vida privada o relaciones familiares que afectan a la fama, crédito o intereses de la víctima.

> *"Si alguien exigiere de otro una cantidad o recompensa bajo la amenaza de revelar o difundir hechos referentes a su vida privada o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés, será castigado con la pena de prisión de dos a cuatro años, si ha conseguido la entrega de todo o parte de lo exigido, y con la de cuatro meses a dos años, si no lo consiguiere".*

En el tercer apartado se intenta acabar con esta práctica rebajando la pena del delito objeto del chantaje en uno o dos grados, (cuando sea inferior a dos años de prisión) para así incentivar a la víctima del chantaje a que denuncie al chantajista.

Junto a estas amenazas la regulación incluye otras previsiones en relación a la violencia de género pero que quedan más alejadas de los delitos informáticos.

En conclusión, la relevancia para los delitos informáticos la da la especial protección que otorga el art.169.1 en su apartado segundo con la previsión en relación a los medios técnicos con los que se puede cometer. Para el resto de supuestos también es aplicable esta característica ya que es una forma más con la que es posible realizar la acción delictiva.

3.2 Coacciones

Se tipifican en el art.172.1 CP:

> *"El que, sin estar legítimamente autorizado, impidiere a otro con violencia hacer lo que la ley no prohíbe, o le compeliere a efectuar lo que no quiere, sea justo o injusto, será castigado con la pena de prisión de seis meses a tres años o con multa de 12 a 24 meses, según la gravedad de la coacción o de los medios empleados".*

Se trata de una acción por la que el autor impide mediante violencia a otra persona que haga algo que no está prohibido o la obliga a realizar lo que no quiere. Entre ambos elementos debe mediar una relación de causalidad.

Para que la conducta se realice en el entorno de la ciberdelincuencia es necesario que la violencia que el tipo requiere sea cometida de forma virtual. Es decir el elemento central de las coacciones es la violencia por la que el autor exige hacer o dejar de hacer algo.

La violencia ha ido evolucionando desde un concepto muy restringido con el que se la veía antes y que requería que fuera física, hasta la actualidad donde se interpreta de forma extensiva incluyendo intimidaciones personales, que pueden venir en el caso de los ciberdelitos desde un chat de una página web donde el autor obliga a la víctima a hacer algo que no quiere por ejemplo.

Como consecuencia de una interpretación tan amplia se hace difícil a veces distinguir entre el delito de coacciones y el de amenazas condicionales, en el elemento de la violencia residirá la diferencia. Un ejemplo de coacciones a través de Internet puede ser el de modificar las contraseñas de un periodista que publica periódicamente en un blog de Internet para que no pudiera acceder al mismo y expresar opiniones que no fueran del agrado del autor.

Para ser sujeto pasivo del delito es necesario que su voluntad quede sometida a la del autor. En el caso de conseguirlo con el empleo de sustancias artificiales no se cumpliría el requisito.

Es además un delito doloso al requerir la intención de someter la voluntad de la víctima, sin que quepa su comisión culposa.

Por último, el delito se consuma en el momento en que el sujeto consigue su objetivo, quedando en grado de tentativa de no hacerlo.

4. Ciberacoso. El nuevo art.172.ter

En la reforma del Código Penal que ha introducido la LO 1/2015 se ha añadido un supuesto específico en el Título VI de los delitos contra la libertad que afecta al ámbito de los delitos informáticos[132].

[132] Junto a previsión del ciberacoso la nueva reforma tiene poca trascendencia en relación a los delitos informáticos, pues además de esa reforma se incluyen cambios como consecuencia de la supresión de las faltas que pasan a ser consideradas como delitos leves. En tal sentido operan las reformas del art.171 y 172 que incluyen sendos párrafos al respecto. Además hay previsiones de relacionadas con matrimonios forzosos

Se trata del supuesto del acoso pero que es llevado a cabo mediante tecnologías de la información y la comunicación, (entre otras posibles formas de comisión).

Se incrimina en el art.172.ter[133], donde se castiga la conducta de quien acosa a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas que el artículo prevé y, de este modo, altera gravemente el desarrollo de su vida cotidiana.

> *"Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:*
>
> *1.ª La vigile, la persiga o busque su cercanía física.*
> *2.ª* ***Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas****.*
> *3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.*
> *4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella".*

Se tipifica de esa forma y de manera específica e independiente el acoso, dándole una redacción más clara que la de la redacción anterior donde ningún supuesto lo contemplaba de forma expresa, lo que obligaba para castigar tales situaciones a acudir a los tipos generales de coacciones o amenazas, así como a los delitos contra la integridad moral.

Para estar ante el citado tipo penal el acoso que sufre la víctima debe ser insistente y reiterado, además debe perturbar gravemente la vida cotidiana de la víctima. Ello plantea problemas interpretativos y habrá que estar al caso concreto.

Además de esos requisitos de reiteración, insistencia y gravedad, es necesario que el modo por el que se desarrolla la conducta y que los cumple sea a través de alguna de las formas que el artículo prevé.

---

o quien obliga a otra persona abandonar el territorio nacional, pero son supuestos en definitiva alejados de la ciberdelincuencia, sin perjuicio del medio por el que se llevaran a cabo.

[133] http://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3440.pdf

La segunda de ellas es en la que aparece el ciberdelito, se trata de una forma de comisión por la que el autor debe establecer el contacto con la víctima mediante un medio de comunicación, a través del cual es por el que se produce el acoso en los términos que enuncia el tipo. Podría desarrollarse por ejemplo mediante el uso de redes sociales en Internet o aplicaciones informáticas instaladas en un teléfono móvil como es el caso de Whatsapp que permite enviar mensajes de texto o imágenes de forma instantánea a cualquier número de móvil.

A pesar de que el delito informático específico se contemple en el número segundo, el resto formas con las que se comete el delito también posibilitan que sean realizadas por medio de Internet, solo que darán lugar a un concurso de delitos con otros regulados en Títulos distintos al de las amenazas y coacciones y que ya han sido objeto de estudio en este trabajo. Por ejemplo el supuesto del número tercero sería común que viniera en concurso con el art.197, pues para obtener los datos personales de la víctima, es posible que el autor haya cometido un delito contra su intimidad.

SECCIÓN OCTAVA: **DELITOS CONTRA LA INTEGRIDAD MORAL**[134]

1. Introducción

Los delitos contra la integridad moral incriminan las conductas de quienes la vulneran, entendida como derecho fundamental del individuo al estar consagrada en el art.15 de la Constitución.

2. Bien jurídico protegido

El bien jurídico protegido es la integridad moral, entendida como el derecho de una persona a ser tratada conforme a su dignidad, sin ser humillada o vejada, cualquiera que sean las circunstancias en las que se encuentre y la relación que tenga con otras personas[135].

Se trata de un bien jurídico que puede entrar en conflicto con el derecho a la libertad de expresión, ya que las opiniones que se vierten amparándose en ese derecho en sí mismas serán lícitas, pero cuando constituyan un ataque contra la libertad moral de otra persona habiéndose manifestado de forma coactiva e intimidatoria darán lugar a un delito contra la integridad moral[136].

Dichos ataques cuando vengan cometidos mediante el uso nuevas tecnología o en soportes informáticos serán tratados como delitos informáticos.

3. Regulación penal

Los delitos contra la integridad moral se regulan en el Título VII del Libro II en los art.173 y siguientes[137].

---

134 La sistemática del Código Penal regula en el mismo Título los delitos contra la integridad moral y las torturas, pero para la categoría delictiva del cibercrimen nos ocuparemos únicamente de la integridad moral en general, donde los autores tienden a ser particulares lo que les permite su comisión por medio de la informática. De esta forma no se expondrá todo el Título VII al contemplar supuestos muy alejados de la posible comisión mediante nuevas tecnologías como las torturas que es cometido principalmente por funcionarios, .o violencia de género.

135 MUÑOZ CONDE, F., *Derecho Penal parte especial*, Tirant lo Blanch, Valencia, 2010, pp. 184-186.

136 STC de 29 de enero de 1982.

137 http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t7.html

El titulo se abre con el tipo básico en relación a la integridad moral que establece:

> *"El que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de seis meses a dos años".*

Esta previsión forma el tipo básico contra la integridad moral donde se incrimina a cualquiera que infrinja un trato degradante grave en otra persona. No define lo que se entiende por trato degradante dejando por tanto una cláusula abierta que genera problemas de interpretación desde el punto de vista del principio de legalidad.

Se viene entendiendo que ello lo forman las acciones que sometiendo o no la voluntad del sujeto pasivo, den lugar a una situación humillante o vejatoria. Todo ello de forma grave, para lo que habrá que estar a las circunstancias concretas.

Este delito será considerado como ciberdelito cuando la conducta por la que se humilla o veja a otra persona se lleve a cabo por los cauces de un soporte informático, por ejemplo mediante insultos continuos que reciba un compañero por parte de otro mediante Whatsapp.

No obstante el tipo penal es bastante residual ya que se aplica cuando la situación no pueda encuadrarse en otro tipo que lo prevea más específicamente, de forma más grave o cuando a pesar de estar previsto en otro tipo no lo esté con la gravedad adecuada. Podría aplicarse en tales casos el concurso entre ellos.

Junto a esta previsión genérica se contemplan otros dos supuestos ligados a la vulneración de la integridad moral.

En primer lugar el acoso laboral e inmobiliario, de los que solo el primero tiene un interés mayor para la categoría de los ciberdelitos.

> *"Con la misma pena serán castigados los que, en el ámbito de cualquier relación laboral o funcionarial y prevaliéndose de su relación de superioridad, realicen contra otro de forma reiterada actos hostiles o humillantes que, sin llegar a constituir trato degradante, supongan grave acoso contra la víctima".*

Es una situación similar en la que no es preciso un trato degradante sino que basta con un grave acoso para la víctima en el entorno de la situación concreta laboral o funcionarial.

De realizar el acoso mediante instrumentos como teléfonos móviles, redes sociales o similares se estaría en la categoría de delito informático.

Además se incluye otro supuesto similar para cuando la víctima sea o haya sido cónyuge del autor o le ligara una especial relación de afectividad.

> *"El que habitualmente ejerza violencia física o psíquica sobre quien sea o haya sido su cónyuge o sobre persona que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia, o sobre los descendientes, ascendientes o hermanos por naturaleza, adopción o afinidad (…)".*

Se trata de un supuesto incluido por la LO 1/2004 que otorga protección a todos los sujetos que el tipo reconoce, pero no solo frente a la violencia física, sino también la psíquica que puede proceder de vejaciones mediante dispositivos móviles.

El supuesto y al igual que sucedía antes, generalmente entrará en aplicación por medio de un concurso con amenazas, coacciones…

Finalmente en la última reforma del Código Penal de marzo de 2015 no se incluyen previsiones específicas en los delitos contra la integridad moral vinculados a la ciberdelincuencia.

SECCIÓN NOVENA: **DELITOS CONTRA EL ORDEN PÚBLICO**

1. Conceptualización

Los delitos contra el orden público constituyen un conjunto de conductas orientadas a proteger la tranquilidad o la paz en las manifestaciones colectivas de la vida ciudadana[138]. Por ello la delimitación de su bien jurídico es muy difícil de aprehender al ser muy confuso, pues el orden público es demasiado intangible.

Se regulan en el Título XXII del Libro segundo del Código Penal en los artículos 544 y siguientes[139]. La sistemática del Código diferencia estos delitos de los delitos contra la Constitución a pesar de que en Códigos anteriores habían estado unidas. De esta forma el orden público protegido en este Título se reduce al ámbito de las manifestaciones de la paz pública en las relaciones sociales y políticas, al incluir también los delitos de terrorismo.

Entre las conductas que se incriminan en los citados artículos destacan especialmente las de sedición, atentados contra la autoridad y desordenes públicos, (además de otras vinculadas con la tenencia de armas y explosivos, así como del terrorismo). Todas ellas tienen en común que castigan actos que vulneran el libre y pacífico ejercicio de los derechos fundamentales. Se persigue garantizar en último término la tranquilidad para el disfrute de los mismos, sin alteraciones, coacciones…

2. Especial referencia del nuevo artículo 559

Las conductas descritas son llevadas a cabo mediante comportamientos activos que requieren una presencia física y simultanea del sujeto activo y pasivo, por lo que en principio serían ajenas a la ciberdelincuencia. Pero con la reforma del Código Penal introducida el pasado mes de marzo mediante la LO 1/2015 se ha modificado el art.559 dentro del Capítulo dedicado a los desórdenes públicos[140]. Ahora en su nueva redacción se

[138] MUÑOZ CONDE, F., *Derecho Penal Parte Especial*, Tirant lo Blanch, Valencia, 2010, pp. 883-884.
[139] http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t22.html
[140] http://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3440.pdf

añade una conducta que incrimina los actos preparatorios a estos delitos que hayan sido realizados mediante medios de distribución o difusión.

> *"La distribución o difusión pública, a través de cualquier medio, de mensajes o consignas que inciten a la comisión de alguno de los delitos de alteración del orden público del artículo 557 bis del Código Penal, o que sirvan para reforzar la decisión de llevarlos a cabo, será castigado con una pena de multa de tres a doce meses o prisión de tres meses a un año".*

El ámbito en el que se encuadra el artículo es el de los desórdenes públicos, estrechamente vinculados con la esencia del orden público al ser su finalidad la protección de la tranquilidad en las manifestaciones colectivas de la vida ciudadana.

Como ha establecido el Tribunal Supremo en la Sentencia de 1 de febrero de 1972 *el desorden, en sentido literal, es la alteración del ritmo normal de la vida ciudadana, que perturba el desenvolvimiento práctico de las actividades públicas.* Se pretende con ello proteger la paz o tranquilidad de la vida pública. Este fin aunque es común en el resto de delitos de este Título, como los atentados, resistencia o desobediencia, se ve de forma más evidente en los desórdenes.

El artículo lo que incrimina es la actitud previa a cometer los desordenes, el comportamiento de quienes los promueven mediante medios de difusión o distribución, incitando de esa forma a cometer los delitos que el capítulo establece, concretamente los del art.557.bis. Este artículo a su vez ha sido también introducido en la misma reforma de 2015 constituyendo una agravante del tipo básico del art.557 en materia de desordenes públicos.

> Los art.557 y 557.bis forman respectivamente el tipo básico y agravado en los delitos de desórdenes públicos, y son a los que el art.559 se refiere al castigar su incitación a través de cualquier medio para cometerlos.
>
> El art.557 castiga la conducta de quien actuando en grupo o individualmente pero amparado en él, alterare la paz pública ejecutando actos de violencia sobre las personas o sobre las cosas, o amenazando a otros con llevarlos a cabo.
>
> Esta conducta se agrava en el art.557.bis cuando se lleve a cabo por medio de armas o instrumentos peligrosos; objetos contundentes o susceptibles de explotar o generar incendios; en el desarrollo de una manifestación o reunión numerosa; en actos de pillaje; mediante abuso de autoridad cuando sea cometido por un funcionario y con la ocultación del rostro o circunstancia análoga.

El art.559 lo que hace es castigar a quienes haciendo uso de *cualquier medio,* inciten a realizar las conductas de art.557.bis. Ello no deja de ser un acto preparatorio del art.557, pero que ahora con la nueva regulación queda tipificado, incluso aunque posteriormente los desórdenes no se llevaran a cabo.

Por la expresión *cualquier medio de distribución o difusión pública* a pesar de lo ambiguo del concepto se pueden entender todas las tecnologías de la información y de la comunicación, como Internet o la aplicación para dispositivos móviles Whatsapp por ejemplo. Estas permiten la rápida propagación del mensaje en poco tiempo haciendo del tipo un delito informático de peligro ante la realización de los posibles desórdenes a los que alientan.

CAPÍTULO II. **CONVENIO DEL CONSEJO EUROPEO SOBRE CIBER DELINCUENCIA DE 2001**

1. Concepto y ámbito de aplicación

El Convenio sobre Cibercriminalidad de Budapest o "Convención sobre Delitos Informáticos" o "Convenio sobre Ciberdelincuencia" es un acuerdo internacional por el que los Estados firmantes regulan a nivel global los aspectos más relevantes de los delitos informáticos tratando aspectos penales, procesales y de cooperación internacional.

De esta forma en un único instrumento se consigue proporcionar un marco legislativo supranacional contra el fenómeno de la ciberdelincuencia (cuya virtualidad precisamente es la posibilidad de actuar simultáneamente en varios estados diferentes), y aumentar la eficacia a la hora perseguir estos delitos y de darles una solución homogénea en todos los Estados.

Pretende por ello garantizar una armonización penal y procesal de las diferentes incriminaciones que desde el Derecho interno puedan proponerse, constituyendo de este modo un pilar fundamental que sirve de sustento a las legislaciones nacionales al comprender aspectos de Derecho penal, procesal e internacional.

Su adopción se produjo el 8 de Noviembre de 2001 por el Consejo de Europa, presentándose en Budapest el día 23 de este mismo mes. Finalmente entró en vigor el 1 de julio de 2004.

No obstante es un instrumento internacional que no es directamente aplicable u obligatorio en los Estados miembros hasta que ellos voluntariamente no lo adopten, pues el Convenio se limita a enunciar normas generales contra la delincuencia informática que no son de aplicación directa ni siquiera en los países que han firmado el texto, debiendo adaptarlo a su legislación interna. En el caso español este hecho se produjo en 2010 cuando el 17 de septiembre se publicó el Convenio en el Boletín Oficial del Estado entrando en vigor el 1 de octubre de ese mismo año[141].

[141] http://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

Como consecuencia de dicha adopción España ha tenido que hacer sucesivas reformas para adaptar su legislación interna al contenido del Convenio.

En este sentido y fruto de obligaciones internacionales similares, España ha tenido que realizar reformas como la de este año introducida mediante la LO 1/2015. Ámbitos como el relativo a la libertad sexual no cumplían con todos los contenidos mínimos que establece el Convenio en relación a la protección de menores.

2. Contenido

El Convenio contempla previsiones específicas para los diferentes tipos penales relacionados con la ciberdelincuencia, aunque la mayoría de ellos ya están previstos en las propias legislaciones internas de manera similar.

El Convenio comienza destacando la necesidad de una protección eficaz hacia la sociedad frente a la ciberdelincuencia tras los cambios sufridos por la digitalización y globalización de las redes informáticas. Ello requiere una lucha efectiva por medio de la cooperación internacional reforzada, rápida y eficaz en materia penal que facilite la detección, persecución e investigación de los delitos tanto a nivel nacional como internacional.

Como antes se señaló, el Convenio se ocupa principalmente de dos ámbitos, por un lado cuestiones relativas al Derecho penal sustantivo, material, al incluir una serie de conductas ilícitas llevadas a cabo mediante instrumentos telemáticos; y por otro incluye aspectos procesales. Finalmente incluye una serie de disposiciones acerca de la cooperación internacional en materia de ciberdelincuencia.

Para llevarlo a cabo, el Convenio cuenta con 48 artículos que se estructuran a lo largo de cuatro Capítulos y que a su vez comprenden diferentes Secciones y Títulos. El primero de ellos regula cuestiones generales y definiciones; el segundo aborda el núcleo duro del Convenio al incluir todos los aspectos penales y procesales; el tercero prevé cuestiones de cooperación internacional; y el último es dedicado a cuestiones finales.

La parte referente al Derecho penal se recoge en el Capítulo II en su primera Sección entre los artículos 2 y 13. En ella se detallan los delitos informáticos en particular pero redactados a modo de recomendaciones que los Estados deben incluir en su legislación.

Lo que se pretende en estos artículos es armonizar la legislación penal entre los Estados firmantes para que en ellos sean punibles las mismas conductas de carácter informático. Sin embargo la mayoría de conductas que en ellos se incluye es similar a la que aparece en nuestra legislación mucho antes de la entrada en vigor del Convenio.

- Dentro de la Sección I dedicada a aspectos penales el primer Título entre los artículos 2-6 regula los delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos. Engloba delitos contra la intimidad, descubrimiento y revelación de secretos, así como el delito de daños informáticos.

    - En primer lugar figura el acceso ilícito, doloso y sin autorización, a todo o parte de un sistema informático, (art.2).

    - En segundo lugar se menciona la interceptación ilícita, dolosa sin autorización, mediante medios técnico, de datos informáticos en el destino, origen o interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos, (art.3).

    - En tercer lugar prevé los atentados contra la integridad de los datos, es decir los daños, borrados, deterioros, alteraciones o supresiones dolosas sin autorización de datos informáticos, (art.4). Es un supuesto contemplado en España dentro del delito de daños.

    - En cuarto lugar incluye los abusos contra la integridad del sistema, es decir la obstaculización grave, deliberada e ilegitima del funcionamiento de un sistema informático mediante las conductas anteriores, (introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos), (art.5).

  El art.6 cierra esta primera Sección requiriendo a las partes a que tipifiquen conductas tales como la producción, venta y obtención para la utilización o difusión de programas informáticos, asi como contraseñas, códigos de acceso o datos informativos. Incluso prevé castigar la mera posesión de todos estos elementos.

- El Título segundo en los art.7 y 8 regula las falsificaciones y las estafas informáticas.

    - En primer lugar el art.7 cuando habla de falsificación informática se refiere a la conducta de quien introduce, altera, borra o suprime de forma dolosa datos informáticos no auténticos para que sean tomados o usados a efectos legales como auténticos.

    - Posteriormente el art.8 en cuanto al fraude regula la conducta de quien cause un perjuicio patrimonial en otro mediante cualquier introducción, alteración, borrado

o supresión de datos informáticos; así como mediante cualquier interferencia en el funcionamiento de un sistema informático.

- El Título tercero se dedica a las infracciones relativas al contenido, dentro de las cuales únicamente regula los delitos de pornografía infantil en el art.9.

  El concepto de pornografía infantil es bastante amplio al considerar como tal a todo material pornográfico que represente de manera visual a un menor desarrollando un comportamiento sexual explícito; a una persona que aparezca como un menor desarrollando un comportamiento sexual explícito; o imágenes realistas que representen a un menor desarrollando un comportamiento sexual explícito. De este modo el comportamiento de quienes no son menores pero aparentan serlo sería constitutivo de delito.

  Como vemos, tal definición se asemeja bastante a la que ha introducido en la legislación española la LO 1/2015 en el art.189 CP donde incluye hasta este último supuesto, al que nos referíamos como *pseudo pornografía*.

  El artículo castiga la mera posesión, producción, difusión, ofrecimiento o puesta a disposición dentro del ámbito punible. Y se cierra proponiendo a las partes que pongan un límite mínimo en 16 años para lo que sería considerado como menor, una cifra también en la línea de la reciente reforma penal española.

- El Titulo cuarto en el art.10 contempla delitos contra la propiedad intelectual y derechos afines, donde se incluyen acciones que la infrinjan de acuerdo a las legislaciones nacionales así como internacionales en materia de propiedad intelectual, haciendo mención expresa de diferentes instrumentos como el Convenio de Berna (que protege obras literarias y artísticas) y el Tratado de la Organización Mundial de la Propiedad Intelectual.

- El último Título relativo a la parte penal que contiene el Convenio habla entre los art.11 y 13 de otras formas de comisión incriminando la tentativa deliberada a realizar cualquiera de las acciones previamente estipuladas, así como la complicidad para llevar a cabo los mismos fines.

  Finalmente prevé responsabilidades para las personas jurídicas según sean o no sujetos activos del delito en las legislaciones nacionales.

El contenido de esta parte es bastante completo, pues comprende la mayoría de tipos penales en materia de ciberdelincuencia, logrando una fuerte armonización a nivel europeo. Sin embargo el problema que plantea es la falta de obligatoriedad de tales disposiciones, pues en ningún lado del Convenio se regulan las consecuencias de la falta de

adaptación de tal normativa a la legislación interna de un país, ni la potestad de un órgano jurisdiccional para sancionar tales actos[142].

Tras esta primera Sección con un carácter propio del Derecho penal se abre una segunda Sección que contempla aspectos puramente procesales entre los art.14-22.

> Los artículos de esta parte se remiten a las legislaciones nacionales para que estipulen el procedimiento penal acorde a la persecución de estos delitos así como la obtención de pruebas, (art.14). Todo ello debe respetar los derechos humanos y libertades fundamentales tanto internas como del Consejo de Europa y Naciones Unidas, (art.15).
>
> Además permite que las autoridades establezcan ficheros donde almacenen datos electrónicos específicos hasta un máximo de 90 días siempre que los datos puedan ser susceptibles de pérdida o modificación, (art.16). E incluso incluye previsiones para que dichas autoridades puedan ordenar a las personas presentar datos que tengan en su poder o equipos informáticos, así como a los proveedores de los datos o servicios similares pudiendo quedar todo ello almacenado en un registro, (art.18).
>
> Finalmente permite a los Estados realizar grabaciones en la red en tiempo real por las propias autoridades o proveedores relativas a estos delitos y permite su intervención cuando circule entre particulares, (art.20). También prevé poder confiscar los datos y realizar copias de los mismos o hacerlos inaccesibles al público en general, (art.19).
>
> Para concluir se regula la jurisdicción competente para tales delitos, remitiéndose a los Estados y que sean estos los que establezcan quien conocerá de los delitos cuando se cometan en su territorio, aplica por tanto el principio de territorialidad, (art.22). También alude a supuestos más problemáticos en casos de que sea cometido a bordo de buques, aeronaves o por sus nacionales en lugares donde otros Estados no son competentes.

Finalmente el tercer pilar sobre el que gravita el Convenio es el relativo a la cooperación internacional, a lo que dedica los art.23 a 35.

> Los artículos de esta Sección contienen una serie de principios relativos a dicha cooperación proporcionándose entre sí la ayuda necesaria y basado en los principio de extradición, en el de asistencia mutua para las obligaciones que sean requeridas y en el de información espontanea, donde las partes pueden comunicar sus investigaciones a otros Estados para facilitar la persecución de otros delitos.

[142] DE LA MATA BARRANCO, N. J.; PÉREZ MACHÍO, A. I.; "La normativa internacional para la lucha contra la cibercriminalidad como referente de la regulación penal española"; en: *Derecho penal informático,* Aranzadi, Navarra, 2010, p.130.

> Junto a ello se regulan procedimientos específicos sobre la asistencia mutua y colaboración para lo que cada Estado deberá designar una autoridad central para su comunicación reciproca que será la encargada de recibir las solicitudes de otros Estados.
>
> Tales principios quedan restringidos a la confidencialidad a la que puedan estar sometidos según sus legislaciones.
>
> El Convenio se cierra con previsiones acerca del traspaso de datos y su acceso entre países para que uno pueda acceder a otro, incluso en tiempo real.
>
> Para garantizar los compromisos que se adoptan en el Convenio se crea una Red 24/7 que implica que cada Estado deberá designar un punto de contacto que esté localizable los 7 días de la semana, las 24 horas del día, para poder facilitar el contacto entre países y autoridades así como las investigaciones relativas a estos delitos informáticos.

Se trata de un Convenio muy completo que regula todos los aspectos sustantivos en relación a la ciberdelincuencia sin que sea necesario acudir a otros instrumentos, lo que proporciona una unidad en la materia a nivel internacional. Garantiza las medidas necesarias para lograr una persecución, investigación y sanción eficaz de todos estos delitos.

Es realmente útil en el seno de la ciberdelincuencia, pues son delitos con un carácter supra estatal, es decir a menudo los autores se encuentran en un país diferente al que desarrollan la conducta delictiva, lo que ocasiona numerosos problemas de cara a su persecución, investigación y detención del responsable. Por ello todas las medidas orientadas a la cooperación supra estatal deben ser recibidas con agrado siempre que los Estados se vinculen estrechamente con el Convenio y busquen implicarse en la materia.

CAPÍTULO III. **CIBERTERRORISMO**

1. Concepto, caracteres y alcance

En el Capítulo VII del Título XXII del Libro II del Código Penal, "de las organizaciones y grupos terroristas y de los delitos de terrorismo", se regulan todas las conductas ilícitas relacionadas con el terrorismo.

Desde 2010 se ha introducido al comienzo del Título una nueva Sección primera denominada "de las organizaciones y grupos terroristas", que comprende los art.571 y 572[143]. En ellos se proporciona el concepto de tales grupos para posteriormente, a partir del art.573, regular específicamente los delitos de terrorismo que cometen sus miembros. Además con la introducción de esa nueva Sección se consigue diferenciar mejor entre lo que se entiende por organización terrorista y criminal, regulada esta última en el Capítulo anterior, el sexto.

El concepto de organizaciones terroristas le proporciona el nuevo art.571 que establece: "*A los efectos de este Código se considerarán organizaciones o grupos terroristas aquellas agrupaciones que, reuniendo las características respectivamente establecidas en el párrafo segundo del apartado 1 del artículo 570 bis y en el párrafo segundo del apartado 1 del artículo 570 ter, tengan por finalidad o por objeto la comisión de alguno de los delitos tipificados en la sección siguiente*[144]*".*

Por tanto el precepto no da directamente el concepto sino que se remite al Capítulo dedicado a las organizaciones criminales así como a la siguiente Sección en cuanto a la finalidad de tales organizaciones.

[143] Este último artículo ha sido introducido en esta Sección tras la reforma de los delitos de terrorismo llevada a cabo por la ley 2/2015, pues en la anterior redacción pertenecía a la segunda Sección que el mismo artículo abría denominada "de los delitos de terrorismo", y que ahora comienza con el art.573.

[144] En la redacción actual el citado art.570 omite hacer referencia a la finalidad que deben tener tales agrupaciones remitiéndose en bloque al nuevo art.573 que las enumera. Antes se aludía a la subversión del orden constitucional o la alteración grave de la paz pública, que ahora se encuadran dentro de las múltiples finalidades que tipifica el art.573.

En relación al concepto de lo que el Código entiende por organización terrorista se debe acudir al art.570.bis.1 y 570.ter.1 donde se regulan las organizaciones criminales. En dicho artículo se establece que tal organización es la formada por dos o más personas que tienen un carácter estable o por tiempo indefinido, en las que sus miembros se reparten las tareas o funciones de manera concertada y coordinada.

Este concepto se completa con la finalidad establecida en el art.573, pues las organizaciones antes descritas para que se consideren como terroristas deben perseguir alguno de los fines en él descritos, estos son[145]:

- Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.
- Alterar gravemente la paz pública.
- Desestabilizar gravemente el funcionamiento de una organización internacional.
- Provocar un estado de terror en la población o en una parte de ella.

Como se desprende de las finalidades anteriores, lo que diferencia una organización criminal de una terrorista es que estas últimas están afectadas por un elemento teleológico, pues sus actividades delictivas deben ir orientadas a alcanzar alguna o varias de las finalidades que el precepto señala.

Una vez establecido el concepto de organización terrorista y su diferencia con las organizaciones criminales hay que referirse a lo que entiende el Código Penal por terrorismo. Para ello en la segunda Sección del Capítulo VII se regulan específicamente los delitos de terrorismo entre los art.573 y 580.

El terrorismo es una forma de criminalidad organizada que se desarrolla dentro del seno de una organización terrorista concreta y que persigue una especial finalidad política, constitucional o social, que se caracteriza por disponer de una amplia gama de medios

[145] Las dos últimas modalidades constituyen una novedad al ser introducidas en el art.571 CP como consecuencia de la reforma que ha sufrido todo el Título tras la LO 2/2015, pues con anterioridad a tal reforma solo las dos primeras hacían que la conducta de una organización criminal se considerara como terrorista, de este modo se amplían los supuestos en que se considera que tales organizaciones son terroristas.

financieros que la permiten sufragar las actividades ilícitas que la propia organización realiza[146].

En suma, constituye una modalidad delictiva, violenta y organizada que persigue la desestabilización del sistema democrático y las bases sobre las que éste se asienta. El concepto definitorio que lo distingue del resto de figuras es la búsqueda de una o varias de las finalidades concretas del art.573 antes expuestas.

Para llevar a cabo tales fines sus modalidades delictivas son amplísimas, pudiendo revestir la apariencia de una multitud de delitos que aparecen en el Código, entre los que destacan los que figuran en el art.573.1 que atentan contra: la vida o la integridad física; la libertad; la integridad moral; la libertad e indemnidad sexual; el patrimonio; los recursos naturales o el medio ambiente; la salud pública; el riesgo catastrófico; incendio; la Corona; de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos; y contra el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías.

Todos ellos seguidos de la finalidad específica del art.573 que caracteriza este tipo de delitos ya que sin ella darían lugar a un delito cometido por una organización criminal sin que pudiera aplicarse el régimen específico del que gozan los delitos de terrorismo.

Tales delitos pueden cometerse de múltiples maneras, pues por la propia esencia de los delitos de terrorismo, al comprender tantas figuras delictivas dispersas por el Código podrán llevarse a cabo según las formas específicas de cada una.

Una de las formas por las que el delito de terrorismo se puede llevar cabo es mediante la red, se trata del ciberterrorismo.

El **ciberterrorismo** constituye una modalidad terrorista en la que los delitos que la organización terrorista comete son llevados a cabo por medio de la red o a través de cualquier tecnología de la información y la comunicación. Por la propia naturaleza del terrorismo las posibilidades delictivas que comprende el ciberterrorismo son limitadas, pues muchos delitos que pueden ser cometidos por organizaciones terroristas requieren un contacto físico con la víctima o con el objeto material del delito, como los que atentan contra la vida por ejemplo, de ahí que su ámbito de aplicación esté limitado.

[146] MUÑOZ CONDE, F., *Derecho Penal Parte Especial*, Tirant lo Blanch, Valencia, 2010, p.921.

En este sentido el art.573 en su última reforma de 2015 ha añadido un segundo párrafo en el que se tipifica expresamente el ciberterrorismo por primera vez sin tener que interpretar si las conductas delictivas son llevadas por la red con la finalidad y autoría concreta de estos delitos.

De este modo el Código contempla expresamente que cuando una organización terrorista, con cualquiera de las finalidades señaladas anteriormente cometa un delito tipificado en los artículos 197 bis y 197 ter y 264 a 264 quater, se considerará igualmente de terrorismo. Tales artículos contemplan los delitos contra la intimidad y los de daños informáticos. Ahora tras dicha modificación del art.573.2 cuando los cometa una organización terrorista serán calificados de ciberterrorismo.

Sin embargo, a pesar de la previsión concreta del art.573 en relación a esas dos figuras delictivas relacionadas con la informática, un delito sería calificado de ciberterrorismo si fuera realizado en la red por una organización terrorista, aunque no fuera de los específicos que el artículo señala.

En general como estamos viendo debido a la propia naturaleza de los delitos informáticos y las exigencias que requieren, se producen cuando se realizan ataques lanzados contra los sistemas de información por parte de una organización criminal de delincuencia organizada.

Con los ataques cibernéticos se pretende atacar infraestructuras vitales de los Estados[147], ya sean organismos públicos o centros que por sus características contribuyen de forma fundamental al desarrollo y sostenimiento del sistema. No obstante para estar ante dicha categoría las acciones deben ir destinadas a vulnerar la sociedad de la información y los principios fundamentales de la libertad y seguridad.

La conducta reviste la apariencia jurídica del delito daños, aunque ya estaba contemplada en el art.573. No obstante como se señalaba antes, junto al delito de daños y al de la intimidad que son los que figuran que dicho precepto podría darse cualquier otro que fuera cometido en la red por una organización terrorista. Sin embargo su ámbito de aplicación queda bastante reducido por la propia esencia de estos delitos ya que es difícil que puedan darse otros supuestos más allá de estos dos, aunque cabría cualquiera como por ejemplo el de amenazas, fraudes informáticos o acoso. Todos ellos mantienen las mismas

[147] Véase MORALES PRATS, F., "Los ilícitos en la red: pornografía infantil y Ciberterrorismo"; en: *El cibercrimen, nuevo retos jurídico-penales, nuevas respuestas político criminales*, Comares, Granada, 2006, pp 273-277.

características que las que se han ido señalando en el trabajo, pero además de incluir los elementos propios de un delito informático ahora se añaden los propios de una organización terrorista.

Finalmente cabe apuntar que al ser las acciones cometidas por organizaciones terroristas y tener esa específica finalidad, se permite que por el principio de especialidad sean enjuiciadas para todo lo referente a las penas y demás especialidades que revisten dichos delitos conforme a los artículos 571 y siguientes del Código Penal relativo a las organizaciones y grupos terroristas y de los delitos de terrorismo.

2. Regulación Penal en materia de ciberterrorismo

La LO 2/2015[148], de 30 de marzo ha reformado los delitos de terrorismo del Código Penal. Esta Ley Orgánica únicamente comprende la modificación del Capítulo VII del Título XXII relativo al terrorismo en sus artículos 571 y siguientes, pues ha sido tramitada de forma independiente a la otra Ley Orgánica (1/2015) que reforma en su conjunto el Código. A pesar de ello ambas leyes entran en vigor el mismo día, el 1 de julio de este mismo año, complementándose perfectamente pues el único ámbito que no contempló la LO 1/2015 fue precisamente el terrorista.

> El hecho de que la reforma introducida por la LO 2/2015 haya sido tramitada de forma paralela e independiente a la reforma completa del Código Penal introducida por la LO 1/2015 obedece a dos razones. En primer lugar a motivos políticos, ya que en este ámbito llegaron a un acuerdo el Grupo Popular y Socialista, lo que no sucedió en el resto de la reforma del Código ya que hubo discrepancias en cuanto a la incorporación al ordenamiento jurídico de la prisión permanente revisable, así como otros aspectos; y en segundo lugar a razones sociales e internacionales tras el incremento en los últimos meses del terrorismo Yihadista y de sus nuevas formas de captación, muchas de ellas vinculadas con las redes donde de forma explícita se publicitan.

La reforma comprende algún cambio legislativo respecto al modelo anterior al endurecer las penas en materia terrorista y contemplar nuevos tipos penales y circunstancias agravantes. Además las finalidades para estar dentro del delito de terrorismo son más amplias, ya que el art.573, tal y como se ha señalado antes, añade nuevos objetivos que deben perseguir las organizaciones terroristas, lo que permite subsumir nuevos comportamientos dentro del delito de terrorismo.

[148] http://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3440.pdf

De entre toda la Ley Orgánica hay dos preceptos que regulan específicamente el ciberterrorismo, los art.575 y art.578. Comprenden dos supuestos que antes si se contemplaban pero de forma mucho más laxa sin entrar a regularlo de forma tan exhaustiva.

El primero castiga las actividades terroristas que se realizan en la red dirigidas al captamiento de nuevos miembros y a su posterior adoctrinamiento y adiestramiento para realizar los fines que las diversas organizaciones persigan.

> *"1. Será castigado con la pena de prisión de dos a cinco años quien, con la finalidad de capacitarse para llevar a cabo cualquiera de los delitos tipificados en este Capítulo, reciba adoctrinamiento o adiestramiento militar o de combate, o en técnicas de desarrollo de armas químicas (…).*
>
> *2. Con la misma pena se castigará a quien, con la misma finalidad de capacitarse para cometer alguno de los delitos tipificados en este Capítulo, lleve a cabo por sí mismo cualquiera de las actividades previstas en el apartado anterior.*
>
> ***Se entenderá que comete este delito quien, con tal finalidad, acceda de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos accesibles a través de Internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines**. Los hechos se entenderán cometidos en España cuando se acceda a los contenidos desde el territorio español.*
>
> *Asimismo se entenderá que comete este delito quien, con la misma finalidad, adquiera o tenga en su poder documentos que estén dirigidos o, por su contenido, resulten idóneos para incitar a la incorporación a una organización o grupo terrorista o a colaborar con cualquiera de ellos o en sus fines.*
>
> *3. (…)*

El artículo contempla el entrenamiento o formación que reciben los futuros miembros de las organizaciones terroristas.

En su primer párrafo se tipifica de forma genérica la conducta que debe realizar el autor y es en el segundo donde expresamente se contempla el delito informático al regular el supuesto en que ese adiestramiento se realice por medio de la red. Se castiga a quien accede a diferentes contenidos on line donde dichas organizaciones se publicitan para conseguir que los usuarios se unan a su red y cometan los delitos que le son propios.

El sujeto activo no es la organización que se publicita, que adoctrina o entrena sino el usuario particular que voluntariamente entra en esas páginas con la finalidad de recibir el entrenamiento pertinente.

En su ámbito subjetivo el delito es doloso, pues el autor debe acceder a tales páginas a sabiendas del contenido que estas tienen y su intención de recibir adoctrinamiento, por lo que la culpa queda excluida de responsabilidad penal. Si bien el dolo debe ir referido a capacitarse o adoctrinarse, por lo que si se accede a una página web que contenga el citado material pero por curiosidad sin tener tal intención, la conducta es impune.

Con anterioridad a la reforma el art.575 se refería únicamente a quienes realizaran delitos contra el patrimonio para así financiar a las organizaciones terroristas. Con la nueva redacción se da una cobertura mucho más amplia para conseguir eliminar toda la publicidad que realizan estos grupos en Internet y así evitar que recluten a nuevos miembros.

> Esta reforma viene precedida de todo el debate por el surgimiento de nuevos grupos Yihadistas que utilizan las plataformas de Internet para atraer a nuevos miembros que posteriormente son destinados a países como Siria donde son definitivamente entrenados, (de ahí la previsión que el tercer párrafo incluye hacia quienes se van de España para colaborar con las organizaciones terroristas o realizar actos terroristas).

La finalidad que persigue el artículo es la eliminación de una fuente tan importante para el reclutamiento de nuevos miembros como es Internet, que permite a las organizaciones difundir su mensaje a todos los rincones del mundo. Si esta finalidad se consigue llevar a cabo las organizaciones terroristas perderían el principal medio por el que se publicitan y el número de personas susceptibles de unirse a ellas en un futuro disminuiría enormemente haciendo más fácil la desaparición de tales grupos.

La segunda reforma en relación al ciberterrorismo se recoge en el art.578 cuya nueva redacción tipifica:

> *"El enaltecimiento o la justificación públicos de los delitos comprendidos en los artículos 572 a 577 o de quienes hayan participado en su ejecución, o la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares, (…).*

> *2.* ***Las penas previstas en el apartado anterior se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo mediante la difusión de servicios o contenidos accesibles al público a través de medios de comunicación, Internet, o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información.***
>
> *3. (…).*
>
> *4. El juez o tribunal acordará la destrucción, borrado o inutilización de los libros, archivos, documentos, artículos o cualquier otro soporte por medio del que se hubiera cometido el delito. Cuando el delito se hubiera cometido a través de tecnologías de la información y la comunicación se acordará la retirada de los contenidos.*
>
> ***Si los hechos se hubieran cometido a través de servicios o contenidos accesibles a través de Internet o de servicios de comunicaciones electrónicas, el juez o tribunal podrá ordenar la retirada de los contenidos o servicios ilícitos****. Subsidiariamente, podrá ordenar a los prestadores de servicios de alojamiento que* ***retiren los contenidos ilícitos, a los motores de búsqueda que supriman los enlaces que apunten a ellos y a los proveedores de servicios de comunicaciones electrónicas que impidan el acceso a los contenidos o servicios ilícitos*** *(…).*
>
> *5. (…).*

Se trata del clásico delito de enaltecimiento del terrorismo, consistente en justificar uno de los delitos de esta Sección o en humillar a las víctimas, pero la nueva redacción amplía las conductas punibles de acuerdo a la nueva realidad social. Lo que se persigue es la protección de la víctima a la dignidad de su recuerdo una vez que ha muerto como consecuencia de un delito de terrorismo, así como el derecho de sus familiares a que se les repete por la pérdida y no se aumente el dolor con actos en los que se las menosprecie o humille[149].

El primer párrafo no ha sido modificado respecto el de la versión anterior, manteniendo la protección para la víctima o sus familiares. Pero junto a él se añaden cuatro nuevos párrafos que contemplan en primer lugar una agravante de la pena para cuando esa justificación venga expresada en Internet, en plataformas de difusión masiva o en general en cualquier tecnología de la información y la comunicación que lo haga accesible al público en general.

[149] MUÑOZ CONDE, F., *Derecho Penal Parte Especial*, Tirant lo Blanch, Valencia, 2010, p.929.

Es por tanto un delito informático específico que se refiere a las nuevas tecnologías de carácter informático de manera expresa al mencionar explícitamente a Internet. En ellas el derecho a la libertad de expresión se ve limitado con otros derechos como al honor, pues las manifestaciones públicas que se producen en el entorno de Internet generan una difusión mucho mayor que en entornos privados, lo que en casos de enaltecimiento del terrorismo provoca un perjuicio mucho mayor en las víctimas.

Solo cabe su comisión dolosa al requerir el delito que el comportamiento con el que actúa el autor vaya referido a justificar o humillar a las víctimas del terrorismo.

Además la nueva redacción del precepto prevé que todo el contenido ilícito que esté en soportes informáticos pueda ser retirado, destruido y eliminado. De este modo se persigue su eliminación total del mundo virtual aunque ello se antoja difícil de lograr debido a que la información que se publica en Internet queda almacenada al mismo tiempo en distintos servidores y buscadores, lo que provoca que no sea suficiente con su eliminación de un lugar concreto.

Para ello además de facultar al juez para que elimine o retire contenidos o servicios ilícitos de las propias páginas web en las que se publicó el objeto del delito, se le permite que ordene a los motores de búsqueda que supriman los enlaces que conducen a tales páginas, así como a los proveedores de servicios de comunicaciones electrónicas que impidan el acceso a los contenidos o servicios ilícitos.

En general se puede decir que la regulación va un paso más allá de la anterior, donde solo se aludía al tipo básico del primer párrafo sin incluir previsiones en relación a la red[150], para pasar a regular una dimensión mucho mayor de forma específica como es Internet donde todo lo que se publica tiene una difusión y permanencia mucho mayor que en el mundo físico.

[150] El Código Penal no solo se castiga la justificación o enaltecimiento en los delitos de terrorismo sino también en otros como el de genocidio. Tal disposición la encontramos en el art.607. 2 dentro del Título sobre los delitos contra la Comunidad Internacional, en el Capítulo relativo al delito de genocidio, al establecer *"la difusión por cualquier medio de ideas o doctrinas que justifiquen los delitos tipificados en el apartado anterior de este artículo, o pretendan la rehabilitación de regímenes o instituciones que amparen prácticas generadoras de los mismos, se castigará con la pena de prisión de uno a dos años"*. Se castiga al igual que sucedía en los delitos de terrorismo la difusión por cualquier medio de doctrinas o ideas que justifiquen el delito. Entre los medios que menciona al ser una cláusula abierta cabe incluir Internet como instrumento por el que se distribuye de forma masiva y rápida todas las ideas que el precepto señala.

De este modo se protege a las víctimas de actos terroristas frente a quienes aprovechando el anonimato de Internet y su difusión masiva las ridiculizan o justifican los actos terroristas atentando contra sus sentimientos, el dolor por la pérdida de un ser querido y el respeto a ellas mismas.

Junto a esta regulación estatal desde ámbitos supranacionales también se regula la materia en diferentes Textos internacionales entre los que destaca el Convenio sobre la Cibercriminalidad de 2001 al que antes se hizo referencia.

Los Estados propugnan estas normas para unificar sus sistemas penales contra el terrorismo regulando de forma semejante los tipos penales, la forma de comisión y sus sanciones.

Dentro del Convenio en sus primeros artículos (2-4) se sancionan los accesos ilegales a los sistemas de información así como su intromisión. Se refiere a la primera modalidad de ciberterrorismo relativa a los daños en infraestructuras vitales de los Estados llevado a cabo por organizaciones terroristas.

REFLEXIÓN FINAL

A lo largo de las páginas anteriores se ha tratado de estudiar la regulación básica en materia de ciberdelincuencia de nuestro país. De este modo hemos podido constatar como dicha materia es sumamente compleja y extensa, pues en mayor o menor medida un gran número de tipos penales están afectados por elementos telemáticos, o es posible realizar la conducta prevista por medio de ellos.

Además se observa como la materia está en continuo desarrollo, pues hemos podido apreciar como en los últimos años las reformas del Código Penal han afectado particularmente a los delitos informáticos, incrementándose las conductas punibles en relación a nuevas situaciones que eran impensables hace pocos años.

En este sentido opera la reforma de marzo de 2015, pues una parte de ella está orientada a la lucha contra el cibercrimen, lo que denota una preocupación del legislador de adelantarse a cambios futuros que puedan experimentar las nuevas tecnologías evitando que tales situaciones queden impunes.

Asimismo se ha podido apreciar como desde una perspectiva internacional se ha ido promulgando bastante normativa al respecto, lo que refleja la importancia que desde las Instituciones europeas y mundiales se da a la ciberdelincuencia, pues una de sus principales notas distintivas, como se ha visto, es la facilidad para su propagación y distribución más allá de las fronteras de un país, lo que implica que el problema no sea solo de un Estado, sino de la sociedad en su conjunto estando obligada a poner solución.

Finalmente cabe concluir que la ciberdelincuencia es un fenómeno relativamente nuevo frente al que se está reaccionando convenientemente en la medida en que los Estados se están adelantando al desarrollo de las nuevas tecnologías mediante sucesivas normas tendentes a su prevención. Sin embargo dentro de esta corriente reformista se han introducido dentro del ámbito del Derecho penal ciertas conductas que anticipan su respuesta, incriminando actos preparatorios o meras tentativas, incluso acudiendo a la técnica de los delitos de peligro abstracto. Esta situación provoca en mi opinión una respuesta demasiado enérgica del Estado contra situaciones indirectamente relacionadas con la lesión al bien jurídico protegido, y que vulnera el principio de intervención mínima del Derecho penal.

En este sentido incide especialmente la reforma del Código Penal al contener supuestos donde la lesión o el peligro para la sociedad no es lo suficientemente grave como para justificar la intervención del Derecho penal, pudiendo resolverse tales conductas acudiendo a otros instrumentos de los que dispone el Estado, como la Administración, aunque ello ocasionaría una limitación de los medios de defensa, ya que el Derecho penal es mas garantista que el Administrativo.

Con todo ello se puede decir que la protección que se dispensa frente a la ciberdelincuencia desde el ordenamiento jurídico español es completa, al contener una regulación específica en la mayoría de Títulos del Código en función del bien jurídico protegido. Además es de valorar la dificultad de esta tarea, pues la complejidad a la hora de investigar y perseguir estos delitos es alta, así como la facilidad elusiva del autor. Para ello contamos con organismos especializados desde diferentes sectores de las Fuerzas y Cuerpos de Seguridad del Estado que permiten un desarrollo eficaz del proceso. Además la cooperación de la que dispone España en esta materia es importante habiendo suscrito numerosos convenios al respecto.

De cara al futuro el reto que se presenta para la sociedad es estar más concienciada acerca de estos delitos y ser conscientes de la gravedad que revisten, ya que hay un desconocimiento generalizado en la población que la hace banalizarlo, dificultado a las autoridades su erradicación. De este modo es preciso alertar de tales delitos a la vez que concienciar de lo reprobables que son algunas conductas aparentemente inofensivas pero que atentan contra bienes jurídicos fundamentales y producen una lacra para la sociedad, como es el caso de los fraudes informáticos o el acoso en la red.

En este sentido de nada sirve una adecuada protección penal si las víctimas no saben que lo son y no acuden ante los órganos jurisdiccionales en busca de protección. Se debe acabar con la banalización y la sensación de que lo que se desarrolla en Internet no es trascendente, pues si hay un ámbito en el que las cosas no se olvidan es el telemático.

BIBLIOGRAFÍA

ANARTE BORRALLO, E., "Incidencia de las Nuevas Tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información", en: *Derecho y Conocimiento, Anuario Jurídico sobre la Sociedad de la Información*, Volumen 1, Universidad de Huelva: Facultad de Derecho, 2001.

CHLOCLÁN MONTALVO, J. A.; GONZÁLEZ RUS, J. J.; MATA Y MARTÍN, R. M.; PIÑAR MAÑAS, J. L.; ROMEO CASABONA, C. M.; et al. en: *El cibercrimen, nuevo retos jurídico-penales, nuevas respuestas político criminales*, Comares, Granada, 2006.

CUERDA ARNAU, M.L. "Menores y redes sociales: protección penal de los menores en el entorno digital", *Cuadernos de Política Criminal, núm. 112, I, Época II,* 2014.

DE LA CUESTA ARZAMENDI, J. L.; DE LA MATA BARRANCO, N. J.; ESPARZA LEIBAR, I.; PÉREZ MACHÍO, A. I.; SAN JUAN GUILLÉN, C.; et al. en: *Derecho penal informático*, Aranzadi, Navarra, 2010.

FERNÁNDEZ TERUELO, J., G., *Cibercrimen, los delitos cometidos a través de Internet*, Constitutio Criminalis Carolina, 2007.

GARCÍA ÁLVAREZ P. "El menor como sujeto pasivo de delitos, con especial referencia a los delitos contra la libertad e indemnidad sexual y los cambios en ellos introducidos por el proyecto de Ley Orgánica de 20 de septiembre de 2013", *Revista General de Derecho Penal*, 2013.

GÓMEZ TOMILLO, M., *Libertad de información y teoría de la codelincuencia. La autoría y la participación en los delitos cometidos a través de los medios de comunicación de masas*, Comares, Granada, 1998.

GÓMEZ TOMILLO, M., *Responsabilidad Penal y Civil por Delitos Cometidos a través de Internet. Especial consideración del Caso de los Proveedores de Contenidos, Servicios, Acceso y Enlaces*, 2ª ed., Aranzadi, Navarra, 2006.

MARCHENA GÓMEZ, M., *Intimidad e informática: la protección jurisdiccional del habeas data.* Boletín de información. Ministerio de Justicia e Interior nº 1768, 1996.

MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal,* Edisofer, Madrid, 2001.

MATA Y MARTÍN. R. M., *Estafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago*, Thomson Aranzadi, Navarra, 2007.

MATA Y MARTÍN, R. M., "Infracciones penales con tarjetas de pago", en: *Separata de Infraçoes Económicas e Financeiras*, *Estudos de Criminologia e Direito,* Coimbra Editora.

MENDO ESTRELLA, A., "Delitos y Redes Sociales: mecanismos formalizados de lucha y delitos más habituales. El caso de la suplantación de identidad", *Revista General de Derecho Penal*, 2014.

MIRÓ LLINARES, F., "Cibercrimen y vida diaria en el mundo 2.0. Las teorías del crimen y la oportunidad en ámbitos específicos"*, Centro Crímina para el Estudio y Prevención de la Delincuencia, Universidad Miguel Hernández de Elche,* 2014.

MIRÓ LLINARES, F., *Internet y delitos contra la propiedad intelectual*, Datautor, Madrid, 2005.

MIRÓ LLINARES, F., *La protección penal de la propiedad intelectual en la sociedad de la información*, Dykinson, Madrid, 2003.

MORÓN LERMA, E., *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, Aranzadi, Pamplona, 1999.

MUÑOZ CONDE, F., *Derecho Penal Parte Especial*, 18ª ed., Tirant lo Blanch, Valencia, 2010.

MUÑOZ CONDE, F., GARCÍA ARÁN, M. *Derecho Penal, Parte General,* 8ª ed., Tirant lo Blanch, Valencia, 2010.

TAMARIT SUMALLA, J. M, *La protección penal del menor frente al abuso y explotación sexual. Análisis de las reformas penales de 1999 en materia de abusos sexuales, prostitución y pornografía de menores,* Aranzadi, Navarra, 2000.

ROPERO CARRASCO, J. "Reformas penales y política criminal en la protección de la indemnidad sexual de los menores", *Estudios penales y criminológicos*, vol. XXXIV, 2014.

RUEDA MARTÍN, M. A. "La relevancia penal del consentimiento del menor de edad en relación con los delitos contra la propia imagen", *Revista para el análisis del Derecho*, 2013.

VILLACAMPA ESTIARTE, C., "Propuesta sexual telemática a menores u online child grooming: configuración presente del delito y perspectivas de modificación", *Estudios Penales y Criminológicos,* vol. XXXIV, 2014.