PROGRAMA DE DERECHO E INFORMATICA
LECCION DIEZ.
LOS DELITOS INFORMATICOS

LOS DELITOS DE PROVOCACION SEXUAL, LA DIFUSION, VENTA O EXHIBICION DE PORNOGRAFIA ENTRE MENORES DE EDAD O PERSONAS CON DISCAPACACIDAD-

Castiga el art. 186 la difusión, venta o exhibición de material pornográfico entre menores de edad o personas con discapacidad, lo que unido a que el artículo anterior se refiere en exclusiva a "actos de exhibición obscena", ha llevado a buena parte de la doctrina a entender que los contenidos en el art. 185 son delitos de exhibicionismo, en tanto que los del 186 son delitos de "provocación sexual".
Con ese carácter "de provocación" sexual, el art. 186 recoge ciertos comportamientos relacionados con "material pornográfico" cuando se exhibe, difunde o vende ante menores de edad o discapacitados. El bien jurídico o interés que subyace en la existencia de esta incriminación es la indemnidad sexual de los sujetos pasivos, en la medida en que el material pornográfico que ante ellos se exhibe, se difunde, o se les vende puede afectar a su desarrollo y madurez psicológica sobre todo en el ámbito sexual, e incluso viciar el futuro desarrollo o ejercicio "normal" de su sexualidad.
Elemento esencial del delito es el concepto de material pornográfico, un concepto que como el mismo concepto de pornografía carece de un contenido concreto y suficientemente determinable, y varía según los standards culturales y sociales de cada momento y lugar. Por otra parte, la definición de "pornografía infantil" que se incorpora al número 1 del artículo 189 del CP en virtud de la reforma de 2015, enturbia más que aclara por los términos literales en que recoge hasta cuatro supuestos distintos, algunos de ellos innecesarios por reiterativos con un marcado corte objetivo y en la que falta sobre todo una definición de qué haya de entenderse por "conducta sexualmente explícita". Un determinado material puede considerarse pornográfico cuando, por una parte, su contenido es en su totalidad o su mayor parte provocador o capaz de excitar desde el punto de vista sexual, y por otra carece de cualquier valor "ético, estético o erótico" que pueda justificar su contenido.
La conducta castigada en el art. 186 recoge tres comportamientos específicos: vender, difundir o exhibir. Como puede apreciarse, son conductas que se caracterizan por poner en contacto el material pornográfico con sus destinatarios, y es precisamente esto lo que se castiga. Por ello no debe sorprender que comportamientos como la elaboración, el participar, favorecer o facilitar la producción, etc., de los materiales pornográficos no son punibles. No debe olvidarse que objeto de la norma es preservar la indemnidad sexual de menores e incapaces, lo cual desde la perspectiva que proponen estas infracciones se consigue prohibiendo el contacto entre el material pornográfico y los potenciales sujetos pasivos.

El delito exige dolo, y a tenor de cierta opinión doctrinal, el consabido elemento subjetivo del injusto relativo a la finalidad lúbrica u obscena del autor; de nuevo, nos parece excesivo exigir este tipo de elementos subjetivos, y entendemos que el delito se perfecciona con la consciencia y voluntad de los elementos típicos; ahora bien, en determinados casos dudosos, la existencia demostrada de una cierta intencionalidad puede servir para precisar sus términos (exhibición de fotos

objetivamente obscenas en un quiosco de revistas, fotos que son contempladas por menores.

LOS DELITOS DE "DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS"

"Descubrimiento y revelación de secretos"

"Descubrimiento", que hay que entender como el acceso o toma de conocimiento de datos o informaciones voluntariamente excluidos por su titularidad del conocimiento ajeno o cuyo conocimiento se limita por la autorización de su titular que fija que puede conocerse, quien puede tener tal conocimiento y para que puede utilizarse tal conocimiento. La "revelación" o lo que es lo mismo la difusión o cesión a terceros de tales conocimientos en que lo que supondría una ulterior vulneración de la voluntad excluyente y de "control" de los datos e informaciones por parte de su titular.

Han añadido, paulatinamente nuevas modalidades delictivas relacionadas con la llamada "libertad informática", generando un contenido acrónico. Precisamente, la última reforma del Título, producida por la reforma llevada a cabo por la LO 1/2015, de 30 de marzo ha venido a dar un nuevo y más preciso contenido a la "intrusión" en sistemas de información (hacking).

Los delitos de "descubrimiento" de secretos o datos reservados (artículos 197.1 y 197.2 y los delitos de "revelación" de tales secretos o datos, que se contemplan en los artículos 197.3, y 197.7, introducido como novedad en 2015 y que presenta una modalidad específica de "revelación" o difusión no consentida de imágenes o grabaciones audiovisuales privadas. Estos delitos varían como veremos en atención a su objeto material, que a su vez suponen un distinto nivel de ejercicio del derecho a la intimidad: así se hablará de "secretos" para aquellos datos o informaciones sobre los que su titular despliega en plenitud su voluntad de exclusión de intromisiones ajenas, y de "datos reservados", que serán aquellos sobre los que el sujeto desarrolla su derecho de "control". Los delitos de "intrusión" en sistemas de información, regulados en la actualidad en los artículos 197 bis y 197 ter.

1. Descubrimiento y revelación de datos o informaciones lesivos del derecho a la intimidad.

1. descubrimiento de secretos o datos reservados de carácter personal

Como hemos señalado, la primera modalidad comisiva es el "descubrimiento" de datos o informaciones referidos a un sujeto que ha manifestado que no quiere que sean conocidos o ha limitado quién y para qué puede conocerlos. Se abarca así la intimidad como bien jurídico tanto en su dimensión de derecho de exclusión de intromisiones ajenas (sobre todo en relación con el concepto de secreto), como en su dimensión dinámica o facultad de control de los datos e informaciones personales.

El "descubrimiento" tiene como objeto material, por una parte, los "secretos": datos o informaciones sobre los que su titular ejercita el derecho de exclusión que supone la intimidad en términos absolutos. Se trata por tanto de datos o informaciones, cualquiera que sea su contenido, y el soporte en que se contienen, sobre los que su titular ha manifestado su voluntad de que no sean conocidos o de que sean conocidos sólo por determinadas personas. Su contenido y trascendencia es indiferente, y aunque con mayor frecuencia serán de naturaleza privada, íntima o personal, o

atinentes al honor o la propia imagen no necesariamente tienen que serlo. Prueba de ello es que cuando se trata de informaciones o datos especialmente personales como la ideología, la religión, las creencias, la salud, el origen racial, o la vida sexual del sujeto se impondrá la agravación prevista en el número 5 del artículo 197.
Lo relevante en el "descubrimiento" es que supone una injerencia en el ámbito que otro quiere mantener reservado.
El concepto de "secreto" ha de completarse con un concepto "formalmente" establecido a nivel constitucional cuando el artículo 18.3 declara "se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".
Los datos reservados de carácter personal o familiar que se encuentren registrados. Estos datos no son secretos por que, normalmente, han sido facilitados por su titular, por lo que no hay una exclusión absoluta, pero siendo datos "privados", personales o familiares, y en consecuencia no siendo públicos quedan también sometidos al control de la voluntad de su titular el cual dispone de los mismos determinando qué se conoce, quien puede conocerlo y para qué.

a. <u>El descubrimiento de "secretos" (art. 197.1)</u>

El artículo 197.1. castiga con una pena de 1 a 4 años y multa de 12 a 24 meses "para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación".
La incorporación como objeto material de los mensajes de correo electrónico es una consecuencia lógica y necesaria motivada por el avance de la tecnología, y permite incluir también todo tipo de archivos, ficheros o documentos electrónicos (que pueden agruparse en la expresión "cualesquiera otros documentos").
La conducta ha de realizarse sin consentimiento del titular de las informaciones, que implica la objetiva exclusión en que consiste la intimidad y convierte a la información en "secreto", y a los documentos, papeles, cartas, o efectos personales en privados o íntimos.
La segunda modalidad alternativa de "descubrimiento" de secretos es la interceptación de las telecomunicaciones del sujeto pasivo. Como hemos señalado este supuesto encuentra anclaje en la garantía constitucional del secreto de las comunicaciones, garantía que sólo quiebra en caso de expresa resolución judicial. Con tal declaración el artículo 18.3 de la constitución pone de manifiesto que las comunicaciones son secretas como regla, cualquiera que sea su modalidad, (telefónicas, telegráficas, postales). La interceptación de telecomunicaciones, viene a constituirse en una modalidad específica de "apoderamiento", o de acceso a los datos o informaciones, generalmente interviniendo en el iter comunicativo entre emisor y receptor del mensaje o comunicación. Al igual que en el caso anterior, la conducta se consumará en el momento en que se produce el apoderamiento o acceso a la información, cuando se tiene disponibilidad sobre los datos aunque no se comprendan.
Finalmente, el artículo 197.1 presenta una última modalidad de conducta con carácter residual, en la que se ha intentado incluir cualquier otra forma de "descubrimiento" o acceso a datos o informaciones objeto de exclusión por su titular. En este sentido se castiga el uso de "artificios técnicos" que permitan ese acceso a la esfera privada o íntima, ya sea mediante la "escucha" no consentida de conversaciones, la grabación, transmisión o reproducción de las mismas, o de

sonidos e imágenes o cualquier otra "señal" de comunicación. En todo caso se requiere la utilización de artificios técnicos, idóneos para captar, transmitir, grabar o reproducir imágenes, sonidos o cualquier otra señal de comunicación que pueda ser captada por medios técnicos.

b. Descubrimiento datos personales registrados (art. 197.2)

El artículo 197.2 recoge dos conductas, en principio, similares, relacionadas con "datos reservados de carácter personal o familiar" que se encuentren registrados en cualquier tipo de archivo o registro –de naturaleza material o informática-, público o privado. Datos a los que se accede, de los que se apodera, que se utilizan o modifican por un sujeto, *sin autorización* de su titular de los datos o el responsable de los registros o ficheros y en perjuicio de otros (que podrán ser en general, el titular de los datos o un tercero). La pena asignada, en ambos casos la misma, coincide con la prevista en el artículo 197.1: pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses.
El precepto supone una reacción frente a la proliferación de bancos o bases de datos personales, cada vez más frecuentes en cualquier actividad del ciudadano, y las posibles intromisiones o uso ilícitos de los mismos, posibles infracciones que no constituían delito sino sólo infracción administrativa sobre todo a partir de la L.O 15/1999 de 13 de diciembre de protección de datos de carácter personal. Nos encontramos por lo tanto con unas infracciones que afectan a la intimidad en relación a la denominada *libertad informática*, o *habeas data* y que se manifiesta como esa capacidad de control sobre los propios datos e informaciones.
Objeto material los datos reservados de carácter personal que se encuentren registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo o registro público o privado.
Los datos, además, han de estar registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. La exigencia, aunque prolija en su precisión legal, es en definitiva que los datos reservados de carácter personal se encuentren registrados en ficheros, soportes o archivos.
Se castigan tres conductas materiales distintas. En primero lugar "apoderarse" o " acceder" a los ficheros de datos registrados. "Apoderamiento" cuando se accede, tomando conocimiento de los mismos, a los datos que los ficheros o registros contienen, al igual que entendíamos en relación con los papeles, cartas o documentos del art. 197.1. Completándose por tanto la conducta tanto cuando, sin acceder a los mismos el sujeto se apodera de los ficheros o soportes que los contienen, como cuando, introduciéndose en los registros o ficheros, se toma conocimiento de los datos reservados de que se trate. Junto al apoderamiento o acceso, se castiga también "utilizar" o usar de cualquier forma los archivos, sin acceder a su contenido, o los datos; y modificar es alterar los datos, y con ello, inevitablemente los ficheros o archivos que contienen. En los casos en los que se produzca el acceso a los ficheros o archivos, será frecuente el concurso con los delitos de intrusión informática regulados en los artículos 197 bis y ter.

1.2. Revelación de secretos o datos reservados de carácter personal

La "revelación" de los secretos o datos, revelación que hay que entender como la difusión, la cesión a terceras personas, o el poner en conocimiento de otros, los contenidos referidos a informaciones o datos que se pretenden íntimos o bajo control de su titular.

Revelación literalmente "se hace público", facilita el acceso, se da a conocer a un número determinado o no de personas, de terceras personas, los datos que voluntariamente pretendía excluir de dicho conocimiento su legítimo titular.
Podrán ser autores de la revelación de secretos, personas distintas a quienes realizan el descubrimiento.

a. Difusión o revelación de datos por quien lo descubrió o tuvo acceso a los mismos (art. 197.3 primer párrafo).
b. Difusión o revelación de datos por quien no tomó parte en su descubrimiento.
c. Difusión, revelación o cesión a terceros no autorizada de imágenes o grabaciones audiovisuales privadas obtenidas con consentimiento del sujeto pasivo (art. 197.7). El número 7 del artículo 197 recoge una infracción de nuevo cuño introducida por la LO 1/2015 de 30 de marzo, a efecto de llenar una laguna en materia de protección de la intimidad que con la regulación vigente hasta el momento resultaba atípica, no obstante haber venido convirtiéndose en un fenómeno de cierta frecuencia en loa realidad social: aquellos casos en que el sujeto pasivo consiente en la grabación de unas imágenes o de algún material audiovisual, que se realizan en un ámbito "privado" y propio. *("un domicilio o en cualquier lugar fuera del alcance e la mirada de terceros"),* sin consentir en la divulgación, revelación, difusión o cesión a terceros de la imagen o grabación obtenida.

Por la proliferación de supuestos como el contemplado en relación con el llamado *sexting,* o la denominada "venganza porno" (*porn revenge)* en que como forma de venganza se hacen públicas imágenes íntimas por parte de las ex parejas sentimentales.
Como supuestos agravados y castigados con la pena en su mitad superior, los casos en que los hechos hubieran sido cometidos por el *cónyuge o por persona que esté o haya estado unida al autor por análoga relación de afectividad, aún sin convivencia;* una agravación que se hace extensiva a los casos en que *la víctima fuese menor de edad o una persona con discapacidad necesitada de especial protección o los hechos se hubieran cometido con una finalidad lucrativa.*

1.3. Tipos agravados de descubrimiento y revelación de secretos o datos reservados.

El número 4 del artículo 197, prescribe una pena de prisión de tres a cinco años cuando los hechos descritos en los números 1 y 2 del artículo 197, se cometan *por las personas encargadas o responsables de los ficheros archivos soportes informáticos, electrónicos o telemáticos, archivos o registros,* o bien cuando se llevan a cabo *mediante la utilización no autorizada de datos personales de la víctima.*
Si los datos así contenidos, se hubieran difundido, cedido o revelado a terceros se impondrán las penas *en su mitad superior.*
"Encargada o responsable" de los ficheros, soportes o los datos de que se trate. La causa de agravación radica en que a la vulneración de la voluntad del titular de los datos o ficheros se añade la infracción de deberes de custodia y reserva derivados de la condición del sujeto, pues en todo caso, tal condición de encargado o responsable los hace garantes del cumplimiento de los límites que impone la voluntad del titular de los datos o los archivos. Se trata por tanto de un delito especial.

La segunda causa de agravación, añadida por la reforma de 2015, consiste en la utilización no autorizada por el sujeto activo de datos personales de la víctima. Lo genuino de esta agravación radica en que la utilización de "datos personales" de la víctima son el medio de acceso a los datos o informaciones, o el medio de apoderarse de ello, lo que supone la utilización de un medio fraudulento cercano a la suplantación o usurpación de personalidad, cuando no un auténtico abuso de confianza (en los casos en que las claves, contraseñas, códigos o cualesquiera otros datos personales se conozcan por haber sido confiados por propia víctima del delito).

2. Delitos de "intrusión" en sistemas de información.

Los delitos contenidos en los artículos 197 bis y 197 ter en la nueva redacción que les ha
conferido la reforma por LO 1/2015 de 30 de marzo recogen la nueva versión, sin duda más completa y acorde con las exigencias de normativa supranacional, los delitos de "intrusión" en sistemas de información (art. 197 bis 1), de interceptación de transmisiones no públicas de datos informáticos (art.197 bis 2), y de producción, adquisición o facilitación a terceros de programas informáticos o contraseñas o códigos para facilitar la comisión de delitos de descubrimiento y revelación de secretos o de intrusión o interceptación de sistemas de información.
Todo ello como consecuencia de las exigencias contenidas en la Directiva 2013/40/UE de 12 de agosto en la que estos delitos encuentran fundamentos y justificación.
Estos delitos encuentran su justificación última en la necesidad de limitar y controlar el uso de la informática y los gigantescos medios que facilita su uso y las posibilidades de uso que abre con vistas a futura, para esta forma dar protección a la intimidad personal, en la doble dimensión que venimos desarrollando en cuanto hemos previamente analizado. Y en este caso, con cierta coherencia con el carácter de última ratio del Derecho Penal se pretende imponer limitaciones al acceso informático a sistemas de información, o a los medios por los que tales medios normalmente se utilizan de forma que se pueda evitar la realización efectiva de intromisiones ilegitimas en la intimidad ajena.
La tutela o el interés por tutelar de otros intereses como la seguridad de los sistemas informáticos, o la intimidad del "domicilio" informático o la seguridad de los sistemas, programas, archivos y su privacidad en dicho ámbito. Bien jurídico tutelado en este caso la seguridad del medio informático y la confidencialidad (lo que supone una remisión a la intimidad) de la información que los sistemas de información contienen y transmiten.

2.1. Los delitos de intrusión en un sistema de información o la interceptación de transmisiones de sistemas de información.

El artículo 197 bis, que recibe una más depurada redacción con la LO 1/2015, de 30 de marzo, contiene en sus dos números las dos grandes modalidades de delitos de intrusión –que no "intrusismo"- en un sistema de información que contempla nuestro ordenamiento, dando así cumplida satisfacción a las exigencias de la Directiva 2013/40/UE de 12 de agosto.
En su número primero, castiga con una pena de prisión a seis años al que "por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecida 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".
Lo que se castiga es introducirse en un sistema de información, teniendo con ello acceso a los datos, informaciones o programas que los gestionan, comprendiendo en mi opinión no solo ataques desde internet sino también cualquier otro medio o procedimiento de acceso a un sistema de información o a alguna de sus partes. Es también constitutivo de delito "facilitar" a otro el acceso, el que pueda introducirse en el sistema, si bien, destaca que no se contemple entre las posibles conductas típicas la consistente en consentir a un tercero el acceso, por lo que la conducta de "facilitar" deberá ser entendida en un sistema especialmente amplio, aunque será dudoso si abarca comportamientos omisivos.
Sistema de información, ha de entenderse "todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automatizado de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento".
La intrusión, el acceso o el mantenimiento en el sistema de información ha de hacerse "vulnerando las medidas de seguridad para impedirlo" y "sin estar debidamente autorizado".
El número segundo del artículo 197 bis, castiga con la pena de prisión de tres meses a dos años o multa de tres a doce meses, a quien "*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".*
Con esa consideración, la Directiva 2013/40/UE incorpora esta infracción como exigencia en su artículo 6. Por transmisión de datos informáticos ha de entenderse: "toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función".
Para la comisión y relevancia de la conducta es necesario la utilización de artificios o instrumentos técnicos, para de esta forma burlar los mecanismos de protección de la emisión de que se trate, así no estar debidamente autorizado, cláusula con que se hace referencia tanto a la ausencia de consentimiento del titular o titulares del sistema o sistemas de información, como a la ausencia de causas de justificación que pudieran justificar la realización de la interceptación.

2.2. La facilitación de medios informáticos para la comisión de delitos contra la intimidad.

La última modalidad delictiva introducida por la reciente reforma de 2015 en el marco de los delitos contra la intimidad es la contenida en el artículo 197 ter, que castiga con una pena de prisión de seis meses a dos años ó multa de tres a dieciocho meses al 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 algunos 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".*

El nuevo precepto recoge lo que se ha entendido como un acto preparatorio para la ejecución de los delitos contra la intimidad que hemos analizado, si bien limitados por pura lógica al descubrimiento de secretos o datos reservados de los números 1 y 2 del artículo 197 y a la intrusión en un sistema de información del artículo 197 bis; y ese que lo que se castiga es la producción, tenencia bajo cualquier concepto, o facilitación a terceros de mecanismos o instrumentos especialmente sofisticados y adecuados para la comisión de estos tipos delictivos.

DELITOS RELATIVOS A LA PRESTACIÓN DE SERVICIOS DE ACCESO CONDICIONAL Y A LA MANIPULACIÓN DE EQUIPOS DE TELECOMUNICACIONES Y SU COMERCIALIZACIÓN

La vertiginosa evolución que se produce actualmente en la llamada sociedad de la información y la comunicación viene a condicionar bastantes de las relaciones preestablecidas en el mercado televisivo, de radiodifusión, de servicios interactivos prestados por vía electrónica y de las telecomunicaciones. Han irrumpido en escena una serie de, "servicios a la carta", interactivos, condicionados a la obligación de una contraprestación económica por parte del consumidor final, directamente dependiente del "paquete" de servicios contratados. La regulación administrativa (respecto a la titularidad para ofrecer estos servicios) y mercantil o civil (en cuanto al catálogo de obligaciones y derechos derivados del acuerdo de voluntades por el que se regula la prestación particularizada de estos servicios) no impide el acceso fraudulento a los mismos. Junto a esta modalidad de prestación de servicios se ha ido desarrollando un mecanismo "fraudulento", consistente en la descodificación de determinados mecanismos electrónicos que garantizan el suministro de contenidos previo pago, mediante la utilización de programas informáticos que evitan la contraprestación económica. Algunos pronunciamientos jurisprudenciales recientes han constatado que no todas las conductas relacionadas con ellos tienen cabida en las figuras delictivas tradicionales (estafa informática del artículo 248.2 CP; revelación de secretos de empresa del artículo 270 CP; fraude de telecomunicaciones mediando mecanismo clandestino o revelación -o utilización- de secretos de empresa del artículo 280 CP; son algunas de las figuras delictivas que estando cerca de estos mecanismos, quedan lejos de poder ser aplicados y si en algún caso se ha hecho, ha sido realizando una interpretación más cercana a la aplicación analógica de la forma penal que a la interpretación extensiva de los preceptos penales).

Ante este panorama la Ley Orgánica 15/2003, de 25 de noviembre, ha tratado de plasmar en el nuevo artículo 286 CP estas conductas, dentro de la sección tercera, "de los delitos relativos al mercado y a los consumidores", del capítulo XI, "de los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores", del Título XIII, "delitos contra el patrimonio y el orden socioeconómico", del Libro segundo del Código penal. Independientemente de la crítica que proceda respecto a su contenido, la propia ubicación del precepto no debe ser pacífica. Tal vez una ubicación junto a las defraudaciones hubiera sido más apropiada.

El artículo 286 CP aparece estructurado en cuatro apartados, en los que con una sistemática y redacción inapropiada para una norma penal, se tipifican dos realidades completamente distintas, las cuales sólo pueden encontrar un lazo de unión en la identidad de la pena prevista y la previsión del adelanto del momento de protección a los actos que van a permitir el posterior uso fraudulento de los servicios de acceso codificado o a los servicios de telecomunicaciones. Incluso podría plantearse la

justificación de su tipificación conjunta y entrelazada en la razón de la utilización de programas informáticos para su comisión, lo cuál es cierto sólo relativamente.

En un intento de sistematizar los distintos tipos que abarca el artículo 286 CP resulta el siguiente panorama:

a. Los apartados primero y tercero de la citada disposición se refieren a las conductas relativas a los servicios de radiodifusión sonora, televisión o servicios interactivos prestados a distancia por vía electrónica, de acceso condicional, esto es, las relacionadas con aquellos servicios difundidos que son accesibles –mediante un sistema de acceso condicional- únicamente a los consumidores autorizados, abarcando también los software que permiten los nuevos servicios interactivos, como el pago por película o partido de fútbol, los servicios de comercio electrónico, los juegos interactivos, los servicios profesionales "on line", etc.

b. Por su parte, su apartado segundo tipifica la manipulación del número identificativo de equipos de telecomunicaciones o su comercialización.

c. Por último, el apartado cuarto de dicho artículo 286 CP adelanta el momento de protección a conductas que, a lo sumo, podrían constituir actos preparatorios, en este caso el ámbito típico se extiende tanto a los servicios de radiodifusión sonora, televisión o servicios interactivos prestados a distancia por vía electrónica, de acceso condicional, como a los relacionados con la manipulación de equipos de telecomunicaciones.

1. DELITOS RELATIVOS A LA PRESTACIÓN DE SERVICIOS DE ACCESO CONDICIONAL.

Artículo 286, apartados 1 y 3 CP:

1.- "Será castigado con las penas de prisión de seis meses a dos años y multa de seis a 24 meses el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:

1º. La fabricación, importación, distribución, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier equipo o programa informático, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.

2º. La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1º.

3 .- "A quién, sin ánimo de lucro, facilite a terceros el acceso descrito en el apartado 1, o por medio de una comunicación pública, comercial o no, suministre información a una pluralidad de personas sobre el modo de conseguir el acceso no autorizado a un servicio o el uso de un dispositivo o programa, de los expresados en ese mismo apartado 1, incitando a lograrlos, se le impondrá la pena de multa en él prevista".

2.- DELITOS RELATIVOS A LA MANIPULACIÓN DE EQUIPOS DE TELECOMUNICACIONES Y SU COMERCIALIZACIÓN.

Artículo 286.2 CP: *"Con idéntica pena será castigado quien, con ánimo de lucro, altere o duplique el número identificativo de equipos de telecomunicaciones, o comercialice equipos que hayan sufrido alteración fraudulenta"*
Con la inclusión en el artículo 286.2 CP de esta figura delictiva trata de poner freno a la manipulación y uso fraudulento de equipos de telecomunicación, especialmente de los teléfonos móviles.
Uso de equipos o programas que permitan el acceso a los servicios de acceso condicional o los equipos de telecomunicación

El artículo 286.4 CP dispone lo siguiente: *"A quien utilice los equipos o programas que permitan el acceso no autorizado a servicios de acceso condicional o equipos de telecomunicación, se le impondrá la pena prevista en el artículo 255 de este Código con independencia de la cuantía de la defraudación"*.

DAÑOS INFORMÁTICOS

La ley orgánica 1/2015, de 30 de marzo, reforma en profundidad los delitos de daños informáticos. La reforma no estaba prevista, pero se incorpora en el dictamen emitido por la Comisión de Justicia sobre el Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, como consecuencia de la incorporación en el ordenamiento interno de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, con la que se pretende aproximar las normas de los estados miembros de la Unión Europea en materia de ataques contra los sistemas de información, mediante el establecimiento de normas mínimas relativas a la definición de las infracciones penales y las sanciones aplicables, y mejorar la cooperación de entre las autoridades competentes. Dispone la Directiva, es necesario, "*llegar a un enfoque común respecto de los elementos constitutivos de las infracciones penales introduciendo las infracciones comunes de acceso ilegal a un sistema de información, de intromisión ilegal en el sistema y de interceptación ilegal"*
Estos delitos de daños en los sistemas informáticos de los artículos 264 CP a 264 ter CP tienen su origen en reforma operada en el Código Penal por la Ley Orgánica 5/2010, de 22 de noviembre, que venía a coincidir con el artículo 4 de la Decisión Marco 2005/222/JAI, que es sustituida por la Directiva 2013/40/UE, del Parlamento Europeo y del Consejo, de 12 de agosto, que pretende ser integrada en el ordenamiento interno con la Ley Orgánica 1/2015, de 30 de marzo.

En el artículo 264 CP, se castigan los daños en los sistemas informáticos; en el artículo 264 bis CP se tipifica la obstaculización o interrupción del funcionamiento de un sistema informático; el artículo 264 ter CP castiga una serie de conductas relacionadas con los programas informáticos o las contraseñas que permitan acceder a un programa informático que tengan por objetivo la facilitación de los delitos anteriores; y el artículo 264 quater CP recoge las penas previstas para cuando es responsable del delito la persona jurídica.

.1. Daños en los datos informáticos, programas informáticos o documentos electrónicos ajenos.

El artículo 264 CP, queda redactado como sigue:

<<1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos 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.

2. 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.

3. 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.>>

1.1. Tipo básico

La naturaleza del bien jurídico tutelado, se trata de un delito patrimonial, que se está más cerca de la indemnidad de los datos o de la propia seguridad informática, evaluable económicamente, aunque no requiera una expresa cuantificación para su consumación.
El objeto material del delito serán los elementos lógicos de un sistema informático (ANDRÉS DOMÍNGUEZ, 2011), es decir, aquellos que no pueden ser leídos directamente por el hombre.

La reforma operada por Ley Orgánica 1/2015, de 30 de marzo del delito de daños informáticos (artículo 264.1 CP) se limita a concretar que los datos que de cualquier modo pudieran borrarse, dañarse, deteriorarse, alterarse, suprimirse o hacerse inaccesible, al igual que en el caso de los programas a que se refiere el tipo, deben ser informáticos, además de incrementar el límite máximo de la pena de prisión prevista que pasa de ser de una pena de prisión de seis meses a dos años a seis meses a tres años, como consecuencia de la transposición de la directiva 2013/40/UE al derecho interno.

.1.2. Tipos agravados

La ley Orgánica 1/2015, de 30 de marzo, introduce algunas modificaciones de más calado en el tipo agravado de daños informáticos (artículo 264.2 CP), elevando hasta 5 las circunstancias que fundamentan el tipo agravado del delito de daños informáticos:

- En el apartado tercero se fundamenta la agravación del delito de daños informáticos, cuando *"el hecho hubiera perjudicado gravemente el funcionamiento de los servicios públicos esenciales o la provisión de bienes de primera necesidad"*.

- El apartado cuarto tipifica como modalidad agravada los hechos que *"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"*.
  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"*.

- En el apartado quinto la modalidad agravada adquiere un fundamento procedimental, en tanto que se agravará cuando para su comisión se hubieren utilizado un programa informático concebido o adaptado principalmente para realizar estos delitos o utilizando una contraseña de ordenador; un código de acceso o datos similares que permitan acceder a la totalidad o parte de un sistema de información.

1.3. <u>Agravaciones específicas</u>

Artículo 264.3 CP, *"cuando los hechos se hubieren cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza del tercero"*.

2. Obstaculización o interrupción del funcionamiento de los sistemas informáticos.

La Ley Orgánica 1/2015, de 30 de marzo, en sustitución al anterior artículo 264.2 CP, añade un nuevo artículo 264 bis CP, con la siguiente redacción:

<<1. 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 informáticos ajeno:

a. *realizando alguna de las conductas a que se refiere el artículo anterior*
b. *introduciendo o transmitiendo datos*
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.

2. 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.

3. 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.>>.

El delito consiste en obstaculizar o interrumpir el funcionamiento del sistema informático ajeno, sin estar autorizado. Es decir, se mantiene la ajenidad propia del delito de daños, en este caso respecto de la titularidad del sistema informático, objeto del delito, y la ausencia de autorización del mismo, lo que fortalece su naturaleza patrimonial individual. La conducta exige que la obstaculización o la interrupción sea grave, sin llegar a suponga el borrado, daño, deterioro, alteración, supresión o inaccesibilidad definitiva a los datos informáticos, programas informáticos o documentos electrónicos ajenos, en cuyo caso sería aplicable lo dispuesto en el artículo 264 CP.

Las modificaciones introducidas por Ley Orgánica 1/2015, de 30 de marzo, respecto de la redacción que daba a este delito de obstaculización o interrupción del funcionamiento de los sistemas informáticos la Ley Orgánica 5/2010, de 22 de junio, son los siguientes:

- Respecto del tipo básico, manteniendo en este caso la pena de prisión de seis meses a tres años, además de la remisión a las modalidades de conducta tipificadas en el artículo 264 CP, supone una correlativa ampliación del ámbito típico de acuerdo a lo dispuesto en el apartado anterior:

    - Se incluye la conducta consistente en obstaculizar o interrumpir el funcionamiento del sistema informático, sin necesidad de dañarlo, con la introducción o transmisión de datos, en el apartado b) del artículo 264 bis CP.
    - Se incluye la conducta consistente en destruir, dañar, inutilizar o sustituir un sistema informático, telemático o de almacenamiento de información electrónica, en el apartado c) del artículo 264 bis CP.

1. Incluye una agravación específica cuando se hubiera perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, con la previsión de la pena en su mitad superior, pudiendo alcanzar la superior en grado. Esto es, pudiendo llegar a los cuatro años y seis meses de prisión.
2. Se incrementa la pena de los tipos agravados, con la remisión a lo dispuesto en el artículo 264.2 CP, con la pena de prisión de tres a ocho años y multa del triplo al quíntuplo del perjuicio ocasionado. Sorprende el diferente sistema de determinación de la pena previsto para este artículo 264 bis CP en su modalidad agravada respecto de los tipos agravados del artículo 264 CP, a cuyas conductas remite, si bien, amplía considerablemente la discrecionalidad judicial a la hora de determinar la pena de prisión prevista, de tres a ocho años, mientras que en el artículo 264.2 CP, se prevé una pena de dos a cinco años que podrá llegar a una siete años y seis meses sólo en los casos en los que existirá un perjuicio de extrema gravedad.

3. Se incluye en el artículo 264 bis.3 CP la agravación relativa a 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, con la previsión de la imposición de la pena en su mitad superior, en línea con lo dispuesto en el artículo 264.3 CP, relativo al borrado, daño, deterioro, alteración, supresión o inaccesibilidad definitiva a los datos informáticos, programas informáticos o documentos electrónicos ajenos.

3. conductas relacionadas con los programas informáticos o las contraseñas que permitan acceder a un programa informático que tengan por objetivo la facilitación de los delitos anteriores.
La Ley Orgánica 1//2015, de 30 de marzo, añade un nuevo artículo 264 ter CP, con la siguiente redacción:<<*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.>>*

En este nuevo artículo 264 ter CP, se tipifican expresamente conductas de peligro abstracto, que a lo sumo constituirían actos preparatorios que son elevados a la categoría de delito consumado, reproduciendo íntegramente, con la misma pena, lo dispuesto en el nuevo artículo 197 ter CP, respecto de los delitos "*del descubrimiento y revelación de secretos"*, al que nos remitimos.

4.<u>responsabilidad penal de la persona jurídica</u>

La Ley Orgánica 1/2015, de 30 de marzo, un nuevo artículo 264 quater CP, que se corresponde con el anterior artículo 264.4 CP, relativo a la responsabilidad penal de la persona jurídica, con la siguiente redacción:

<<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.>>

DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL

Desde que el Código penal de 1870 incluyera el artículo 552 CP, entre los delitos de estafa y otros engaños, con una referencia genérica "*a los que cometieren alguna defraudación de la propiedad literaria o industrial"*, esta figura delictiva se ha ido manteniendo en los distintos códigos penales históricos como una modalidad de fraude patrimonial construida, como una norma penal en blanco, , con una remisión normativa genérica a la normativa extrapenal, hasta su novedosa configuración en el Código penal de 1995, en donde se apuesta decididamente por un cambio de estrategia otorgando una tutela penal autónoma tanto de la propiedad intelectual como de la propiedad industrial. Ello no obsta, obviamente, que para al integrar las conductas tipificadas en estos tipos penales sea imprescindible el auxilio de normas específicas civiles y mercantiles relacionadas tanto con la propiedad intelectual como con la propiedad industrial. El auxilio normativo en el marco de la tutela penal de la propiedad intelectual será principalmente respecto de la Ley de Propiedad Intelectual, aprobada por Real Decreto Legislativo 1/1996, de 12 de abril.

Tras las reformas operadas por las Leyes Orgánicas 15/2003, de 25 de noviembre, 5/2010, de 22 de junio y 1/2015, de 30 de marzo, la sección primera del capítulo XI, del Título XIII del Libro segundo del Código penal, queda estructurado de la siguiente forma:

a) Un tipo básico, relativo a la reproducción, plagio, distribución, comunicación pública o cualquier otra forma de explotación económica de una obra o prestación literaria, artística o científica (artículo 270.1 CP)
b) Un tipo asimilado al tipo básico, incluido por Ley Orgánica 1/2015, de 30 de marzo, relativo al acceso o localización a través de internet de obras objeto de propiedad intelectual (las llamadas webs de enlaces) –apartados 2 y 3 del artículo 270 CP-.
c) Un tipo atenuado relativo a la distribución o comercialización ambulante u ocasional (artículo 270.4 CP).
d) Unos tipos relativos a la exportación, almacenamiento o importación de objetos producto del delito (artículo 270.5, apartados c y d).
e) Unos tipos relacionados con las medidas tecnológicas de protección que facilitan su eliminación o elusión (artículo 270.5, apartados c y d).
f) Unos tipos agravados en atención al beneficio obtenido o que se pudiera obtener, a la especial gravedad del delito o a la pertenencia del culpable a una organización o asociación delictiva (artículo 271 CP).

Por su parte, el artículo 272 CP, remite a la Ley de Propiedad Intelectual para determinar la extensión de la responsabilidad civil derivada de la comisión de estos delitos, así como la posibilidad de que pueda decretarse en la Sentencia condenatoria su publicación a costa del infractor.

1. Bien jurídico protegido

La propiedad intelectual tiene por objeto –junto con la industrial- bienes inmateriales (MIRÓ LLINARES, 2015), de carácter intangible, pero evaluables económicamente.

Aún cuando el artículo 20.1.b de la Constitución española reconoce y protege el derecho fundamental "*a la producción y creación literaria, artística, científica y técnica"*, lo que se tutela en el artículo 270 CP es otra cosa diferente a ese derecho fundamental a la creación intelectual, en tanto que la tutela se ofrece al autor de la creación intelectual ya realizada; es decir al derecho de autor comprensivo de los derechos morales y patrimoniales de la obra ya

realizada, que corresponden al creador y que sólo pueden vincularse al derecho de propiedad recogido en el artículo 33 de la Constitución Española.

2. Tipo Básico

El artículo 270.1 CP establece lo siguiente: *"será castigado con la pena 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"*.

La Ley Orgánica 1/2015,de 30 de marzo, ha reformado en profundidad el tipo básico de los delitos contra la propiedad intelectual en una línea expansionista del Derecho penal:

_ De inicio incorpora un aumento punitivo, pasando de una pena de prisión de seis meses a dos años y
multa de doce a veinticuatro meses a una pena de prisión de seis meses a cuatro años y multa de doce a
veinticuatro meses.

_ En la descripción de la conducta típica se incluye la fórmula genérica "o de cualquier otro modo explote
económicamente"; junto con los verbos típicos ("reproducir", "plagiar", "distribuir", o " comunicar
públicamente" que tradicionalmente ya se incluían en línea con la tutela de los derechos de explotación
exclusiva que le reconoce al autor el artículo 17 de la Ley de Propiedad Intelectual).

_ Se cambia la fórmula tradicional en los delitos patrimoniales, *"quien, con ánimo de lucro y en perjuicio
de tercero"*, por una más novedosa y amplia: *"quien, con ánimo de obtener un beneficio económico
directo o indirecto"*.

_ Se amplía el objeto material del delito, incluyendo junto a la *"obra literaria, artística o científica, o su
transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a
través de cualquier medio"; "la 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"*. La referencia a las "prestaciones" ya aparece en la Ley de Propiedad Intelectual, si
bien sin una definición determinada, constituyendo un concepto al que debe dotarse de un contenido diferenciado al de obra, y que viene a ampliar el ámbito del tipo.

3. Tipo asimilado al tipo básico (Web de enlaces)

La Ley Orgánica 1/2015, de 30 de marzo, como novedad, incluye los apartados 2 y 3 del artículo 270 CP, dedicados expresamente a las conductas desarrolladas a través de internet consistentes en proveer el acceso o la localización de obras o prestaciones objeto de propiedad intelectual sin autorización de sus titulares; esto es, la tipificación de las llamadas "Web de enlaces", excluyendo, como dispone el propio preámbulo de la Ley, a quienes realizan "*actividades de mera intermediación técnica, como puede ser, entre otras, una actividad neutral de motor de búsqueda de contenidos o que meramente enlacen ocasionalmente a tales contenidos de terceros"*.

Así, los apartados 2 y 3 del artículo 270 CP disponen lo siguiente:

2. *"La misma pena –prisión de seis meses a cuatro años y multa de doce a veinticuatro meses) 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.*

3. 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".

El nuevo tipo asimila a la explotación económica de la obra o prestación objeto del derecho de propiedad intelectual otras conductas de intermediación lucrativa que, con distinta denominación, han ido desarrollándose a través de internet, y que posibilitaban el acceso de múltiples usuarios a obras protegidas por los derechos de propiedad intelectual, sin que el usuario final tuviera que hacer ningún desembolso económico por dicho acceso, causando un perjuicio a los titulares de los derechos de propiedad intelectual. Se tipifica la conducta de aquellas páginas Web que, sin alojar directamente los contenidos protegidos, contienen enlaces que derivan a un servidor externo de gran capacidad donde las obras se encuentran alojadas, desde donde se pueden descargar o visionar directamente, o bien, activar la descarga a través de un sistema de intercambio de archivos P2P, desde el ordenador de otro usuario.

El problema lo soluciona expresamente el legislador de 2015 incluyendo este nuevo tipo penal asimilado al tipo básico, equiparando a las conductas que directamente suponen una explotación económica ilícita de los derechos de propiedad intelectual de las obras o prestaciones sin el consentimiento de sus titulares o cesionarios, las conductas realizadas a través de los servicios de la sociedad de la información que facilitan el acceso a las páginas Web de contenidos en las que se encuentran ubicados las obras o prestaciones objeto del delito contra la propiedad intelectual. Quedan excluidos expresamente quienes desarrollen actividades de mera intermediación técnica, como puede ser, entre otras, una actividad neutral de motor de búsqueda de contenidos o que meramente enlacen ocasionalmente a tales contenidos de tercero, tales como los motores de búsqueda.

5. Exportación, importación, almacenamiento de productos objeto del delito.

El actual artículo 270.5 CP, en sus apartados a) y b) complementa al tipo básico del apartado primero, incluyendo actividades relacionadas con la exportación, el almacenamiento y la importación de los productos del delito:

"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 intencionalmente estos productos sin dicha autorización, cuando estuvieran destinados a ser reproducidos, distribuidos o comunicados públicamente, tanto si éstos tienen un origen licito 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".

6. Tipos relacionados con las medidas tecnológicas de protección.

Los apartados c) y d) del artículo 270.5 CP recogen otros tipos complementarios de los tipos básicos y atenuados, con la siguiente redacción:

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 ejecuciónartística, 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".

Por su parte el artículo 270.6 CP, en un adelantamiento de la intervención punitiva a fases previa a la facilitación de las conductas delictivas contra la propiedad intelectual, castiga la fabricación, importación, puesta en circulación o posesión con una finalidad comercial un medio para neutralizar los sistemas de protección de los productos objeto de los derechos de propiedad intelectual, con la siguiente redacción:

6. 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”.

7. Tipos agravados.

El artículo 271 CP recoge cuatro tipos agravados, en atención a la especial trascendencia económica del beneficio obtenido o que se hubiera podido obtener, a la especial gravedad de los hechos o de los perjuicios ocasionados, a la pertenencia del culpable a una organización o asociación dedicada a la realización de infracciones de los derechos de propiedad intelectual o en atención a la utilización de menores de 18 años. En concreto dispone lo siguiente:

“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 periodo 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.”*