LA ROBÓTICA Y LA INTELIGENCIA ARTIFICIAL EN LA NUEVA ERA DE LA REVOLUCIÓN INDUSTRIAL 4.0

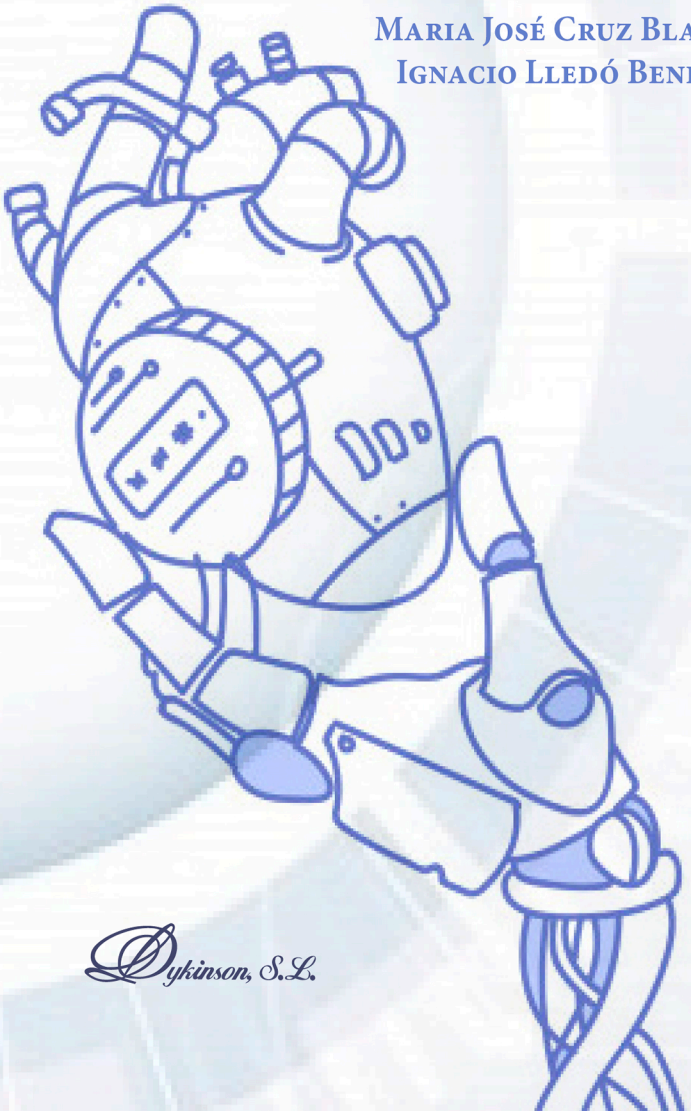
(Los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes)

Directores

Francisco Lledó Yagüe
Ignacio Benitez Ortúzar
Oscar Monje Balmaseda

Coordinadores

Maria José Cruz Blanca
Ignacio Lledó Benito



ACCESO PREMIUM
Libro + ebook

Dykinson, S.L.

Colección
IA, Robots, y Bioderecho

LA ROBÓTICA Y LA INTELIGENCIA ARTIFICIAL EN LA NUEVA ERA DE LA REVOLUCIÓN INDUSTRIAL 4.0

(Los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes)

Colección
IA, ROBOTS, Y BIODERECHO

LA ROBÓTICA Y LA INTELIGENCIA ARTIFICIAL EN LA NUEVA ERA DE LA REVOLUCIÓN INDUSTRIAL 4.0

(Los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes)

Directores

FRANCISCO LLEDÓ YAGÜE

IGNACIO BENITEZ ORTÚZAR

OSCAR MONJE BALMASEDA

Coordinadores

MARIA JOSÉ CRUZ BLANCA

IGNACIO LLEDÓ BENITO

Dykinson, S.L.

Este libro ha sido sometido a evaluación por parte de nuestro Consejo Editorial

Para mayor información, véase *www.dykinson.com/quienes_somos*

El presente trabajo se ha realizado financiado por el Proyecto de I+D+i DERECHO Y MEDICINA: DESAFIOS TECNOLOGICOS Y CIENTIFICOS (DEMETYC) PID2019104868RA-I00 / AEI /10.13039/501100011033.

Editorial DYKINSON, S.L. Meléndez Valdés, 61 - 28015 Madrid
Teléfono (+34) 91 544 28 46 - (+34) 91 544 28 69
e-mail: info@dykinson.com
http://www.dykinson.es
http://www.dykinson.com

ISBN: 978-84-1324-802-8
Depósito Legal: M-20511-2021

ISBN electrónico: 978-84-1377-661-3

Preimpresión por:
Besing Servicios Gráficos S.L.
e-mail: besingsg@gmail.com

Índice

CIBERDELITOS. LA IMPLEMENTACIÓN EN EL ORDENAMIENTO INTERNO DE LOS ACUERDOS INTERNACIONALES EN MATERIA DE CIBERDELINCUENCIA

Ignacio F. Benítez Ortuzar
Catedrático de Derecho Penal. Universidad de Jaén
ibenitez@ujaen.es

1. INTRODUCCIÓN. ACERCA DE LA CIBERDELINCUENCIA

La realidad en la que se ha instalado la llamada sociedad de la información y la comunicación, cada vez más compleja y accesible al mismo tiempo, con la creación de artificios que llegan a actuar con una cierta independencia del ser humano, también va a influir con fuerza en el ámbito propio de la criminalidad. La delincuencia es indisociable de las formas en las que se organiza y desarrolla una determinada sociedad, adaptando sus formas de operar a las posibilidades que ésta les ofrece. En este sentido, la era de la informática, además de facilitar la actividad en múltiples facetas de la información y el conocimiento, permite la aparición de nuevas formas de realización de la actividad delictiva. Los aspectos relacionados con la telemática y la irrupción de Internet como una red de redes de alcance auténticamente global,

permitieron además una inmediatez en el resultado unido a la posibilidad de la distancia en la acción; circunstancias que, en el marco de la actividad criminal y de la eficacia del Derecho punitivo de los Estados, ya advirtieron la aparición verdaderos problemas si se partía de las previsiones jurídicas tradicionales. Realidad que se hace más palpable con la evolución de la tecnología y la implementación del Big data y el mundo de los algoritmos en "aparatos" a los que se les dota de la llamada "inteligencia artificial", con una capacidad de aprendizaje cada vez más autónomo respecto de la actuación de sus creadores y/o de sus usuarios.

Debe observarse, no obstante, desde este momento, que la actividad fraudulenta o criminógena relacionada con la telemática no siempre va a suponer que emerjan nuevos valores sociales a tutelar; es decir, no van a dar lugar a la creación de bienes jurídicos de nuevo cuño. Al contrario, en la mayoría de los casos, por no decir en todos, el bien jurídico tutelado que se ve lesionado o puesto en peligro como consecuencia de la aplicación de los desarrollos tecnológicos es un bien jurídico tradicional, cuya tutela ya es objeto de protección por el Derecho penal. Son las formas de lesión o puesta en peligro de esos valores fundamentales para la sociedad y el individuo las que se ven facilitadas por las innovaciones tecnológicas. Formas de lesividad que, por otra parte, como consecuencia de la taxatividad propia del principio de legalidad penal, no siempre aparecen reflejadas en los tipos que incluyen los Códigos punitivos de los distintos Estados y que han ido dando lugar a cambios legislativos en los últimos años.

En este momento inicial no debe obviarse otra particularidad a la que da lugar la inmediatez del resultado y la distancia en la actividad, en relación a la investigación penal de este tipo de delitos. Al poder actuar en cualquier lugar del mundo desde distancias remotas se obliga a los Estados a realizar un esfuerzo en la cooperación policial y judicial en su persecución, sin la cual, el mejor texto punitivo material sería completamente inaplicable.

Con muchas reservas el Derecho penal liberal se fue adaptando a las complejas estructuras sociales, incluyendo incluso la previsibilidad de la responsabilidad penal de las personas jurídicas, aun cuando ello supone todo un ataque a la línea de flotación del principio tradicional del principio "societas delinquere non potest", y a la eterna discusión acerca de las hipotéticas capacidades de acción y de culpa de estos entes colectivos. El Derecho y, en concreto, el Derecho penal, no puede ser ajeno a la sociedad en la que desempeña sus efectos, y no cabe duda que transcurridas las dos primeras décadas del siglo XXI, la realidad social no puede disociarse de los efectos que el "big data" produce en todas las facetas, también, como no podría ser de otra manera, en el mundo de la delincuencia. El mundo de la inteligencia artificial, con algoritmos que permiten respuestas autónomas a máquinas, que van ampliándose con un aprendizaje autónomo, empieza a abrir -al menos desde planteamientos aún teóricos- grandes interrogantes a los que habrá que ir dando respuestas fiables y ciertas.

Sentada la introducción anterior, lo primero que hay que abordar es la propia nomenclatura de la que se dota a esta tipología delictiva. Afirmando que ni existe ni es fácil que se consensue un concepto unitario perfectamente definido de "delito informático" que incluya todas las modalidades delictivas que tienen en los datos incorporados en los sistemas informáticos o en los propios sistemas informáticos el objeto o el instrumento del delito. Incluso, aún cuando inicialmente parecían acuñarse los términos de "delito informático"[1] o de "delincuencia informática"[2], inmediatamente con perspectiva de permanencia en el tiempo, se intuye que no es aventurado afirmar que el "delito informático como tal no existe"[3]. En realidad, son varias las formas con las que, en muchos casos de modo coloquial, se suele hacer referencia a este tipo de actividad delictiva. Así, podían encontrarse diversas nomenclaturas al respecto, indistintamente utilizadas[4]; por ejemplo: "delito informático", "delito telemático", "ciberdelito", "delito tecnológico", "cibercrimen", o "delito telemático"[5]. Por ello, ya se apuntaba que era más conveniente hablar de ciberdelincuencia o de delincuencia informática o telemática, puesto que de lo que se trata es de estudiar aquellos delitos en particular que se cometen a través de las nuevas tecnologías de la información y la comunicación, por lo que la terminología utilizada no es estrictamente jurídica, sino más bien de referencia[6]. Debe tenerse presente que la actividad realizada con las tecnologías de la información y la comunicación lo que

---

[1] Al respecto, vid. SOLARI MERLO, M.N., "Análisis de los delitos informáticos. una propuesta de clasificación", en *Revista de Derecho y Proceso penal*, n. 60, 2020, páginas 91 y siguientes.

[2] En este sentido, el Decreto del Fiscal General del Estado de 17 de abril de 2007 otorgando delegación expresa en un Fiscal de Sala de primera categoría para la dirección y coordinación de las funciones del Ministerio Fiscal en materia de delincuencia informática".

Al respecto, entre otros, AA.VV., *Delincuencia informática: tiempos de cautela y amparo*, Madrid 2012; DE LA MATA MARTÍN, R., *Delincuencia informática y Derecho penal*, Madrid 2012; DE LA CUESTA ARZAMENDI, J,L./DE LA MATA BARRANCO N.J. (Coords.) *Derecho penal informático,* Madrid 2010; VELASCO NUÑEZ, E./SANCHÍS CRESPO, C., *Delincuencia informática. Tipos delictivos e investigación criminal*, Valencia 2019.

[3] BENITEZ ORTUZAR IF. "Informática y delito". Aspectos penales relacionados con las nuevas tecnologías, en Benitez Ortúzar (dir.) *Reforma del Código penal. Respuestas para una sociedad del siglo XXI*, página 112.

[4] Así, de modo ilustrativo, por ejemplo VELASCO NÚÑEZ, E., en dos artículos coetáneos, en uno de ellos utiliza el término "delitos informáticos" y en otro el término "delitos telemáticos", siendo referidos ambos artículos a la problemática procesal que se plantea en este tipo de delincuencia. "Aspectos procesales de la investigación y de la defensa en los delitos informáticos". La Ley, 2006-3, páginas 1857-1864; y "Cuestiones procesales relativas a la investigación de los delitos telemáticos", Cuadernos de Derecho Judicial, 2006-3, páginas 267-320.

[5] En este sentido SALOM CLOTET, J., señala que "todos ellos no son más que formas o modismos de definir una misma idea o concepto", "La investigación del delito informático en la Guardia Civil", Incorporación de las nuevas tecnologías en el comercio: aspectos legales. Estudios de Derecho Judicial 71, Madrid 2006, página 55.

[6] BENÍTEZ ORTUZAR IF. "Informática y delito"…, ob. cit., 113; GALÁN MUÑOZ, A., El fraude y la estafa mediante sistemas informáticos, Valencia 2004, página 36.

hace es facilitar e incluso realizar tareas que hasta hace poco tiempo eran tarea exclusiva de los seres humanos, y que "ahora los ordenadores, es decir los sistemas electrónicos, tienen la capacidad de reproducir o simular las formas de trabajo propias de la mente humana"[7], con eficacia en distintos sectores de la actividad cotidiana y, también, de la actividad criminal. El propio "Convenio sobre Ciberdelincuencia del Consejo de Europa, firmado en Budapest el 23 de noviembre de 2001", dentro de los "ciberdelitos", separa los "delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos" (entre los que incluye sólo el "acceso ilícito"; la "interceptación ilícita", la "interferencia en el sistema" y el "abuso de dispositivos"), de los "delitos informáticos" (entre los que incluye la "falsificación informática" y el "fraude informático")[8]. Manteniendo una relación de género a especie, siendo -en este sentido- los delitos informáticos solo una parte de los ciberdelitos.

Desde semejante planteamiento, -aún siendo indiferente la denominación "delincuencia informática", "ciberdelincuencia" o "cibercriminlidad"- se va consolidando la denominación "cibercriminalidad", quizá con una perspectiva de utilizar una terminológica más homogénea al mundo anglosajón que por cualquier otra razón ("cybercrime"), como pone de manifiesto el ya séptimo informe sobre Cibercriminalidad en España[9] o la propia "estrategia nacional sobre seguridad 2019"[10], que incluye una definición de "cibercriminalidad", en los siguientes términos: "*El término cibercriminalidad, hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso de hacktivismo*".

Desde un punto de vista sistemático incluso podrían distinguirse dos grupos de ciberdelitos, agrupados en los delitos de resultado y los delitos de medio, refiriéndose

---

[7] CASTILLO JIMÉNEZ, C., "Protección del Derecho a la Intimidad y uso de las nuevas tecnologías de la información"; Derecho y Conocimiento, n. 1, página 35.

[8] Recogiendo en otros apartados los "delitos relacionados con el contenido" (abarcando los delitos relacionados con la pornografía infantil"); y "los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines".

[9] Estudio sobre la Cibercriminalidad en España 2019. Ministerio del Interior. Secretaría de Estado de Seguridad, Madrid 2019. Al respecto, en su página dos afirma lo siguiente: "A tales fines responde la publicación de este VII informe sobre *Cibercriminalidad*, correspondiente a la *delincuencia informática* registrada en el año 2019. Los datos de este informe son los correspondientes a la información estadística que computa la *ciberdelincuencia*….". En tres líneas utiliza de forma indiferente los términos cibercriminalidad, delincuencia informática y ciberdelincuencia.

Por su parte, la Fiscalía General del Estado utiliza el término "criminalidad informática. En este sentido la Instrucción 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías.

[10] Orden PCI/487/2019, de 26 de abril (BOE n. 103, de 30 de abril de 2019).

el primer caso a las conductas que vulneran los sistemas que utilizan tecnologías de la información y los segundos, a las conductas que utilizan las novedades tecnológicas como medio para atentar contra la propiedad, la intimidad, la privacidad o la indemnidad sexual, entre otros bienes jurídicos. En esta línea se pronunciaba también la Estrategia Nacional de Seguridad de 2019, cuando afirma que "*son tres los ámbitos en los que se desenvuelve la lucha contra la cibercriminalidad: i) el ciberespacio como objetivo directo de los hechos delictivos, o de la amenaza; ii) el ciberespacio como medio clave para su comisión; y iii) el ciberespacio como medio u objeto directo de investigación en cualquier tipo de hecho delictivo*". Siendo este tercer ámbito instrumental en la investigación criminal.

Sin embargo, en el ámbito jurídicopenal esta clasificación no es operativa, en tanto que el ataque a los sistemas informáticos en sí mismos alcanza relevancia penal en cuanto éstos contienen una información relevante de personas, empresas, etc, incluyéndose los tipos penales en los respectivos títulos y capítulos del libro segundo del Código penal. El acceso a los sistemas sin más lesividad a bienes jurídicos tradicionales debería quedar al margen del derecho punitivo, salvo que se permita una flexibilidad punitiva en esta parcela de la vida social que sobrepase el principio de intervención mínima[11]. No obstante, la incorporación del artículo 197bis CP por Ley Orgánica 1/2015, de 30 de marzo, sobrepasa dicho límite, tipificando el simple acceso no autorizado al sistema de información violando las medidas de seguridad establecidas para impedirlo.

La imposibilidad de limitar el uso ilícito y fraudulento de las tecnologías de la información y la comunicación es la razón por la que el Código penal español no incluya específicamente un Título o un Capítulo rubricado específico sobre la materia, que podría tener alguna de las rubricas siguientes: "de los delitos informáticos", "de los delitos relativos a la informática", "de los delitos relativos a la sociedad de la información y la comunicación", o "de los ciberdelitos". Tratar de incluir todas las posibilidades delictivas imaginables a través de las tecnologías de la sociedad de la información y la comunicación en una única parte del Código penal, en aras a una mayor organización y sistematización de los tipos penales, conduciría sencillamente al fracaso legislativo.

No obstante, a lo largo del articulado del Código Penal se encuentran diseminados multitud de tipos penales cuya comisión puede ser incluida dentro del término coloquial de "delincuencia informática", "criminalidad informática", "ciberdelincuencia" o "cibercriminalidad", por lo cual, en la descripción de la conducta típica se hace expresa referencia a esta modalidad delictiva, cuando con la redacción tradicional no se incluía (como ocurre, por ejemplo, con los delitos contra la intimidad, en los llamados daños informáticos o en determinados delitos contra la indemnidad sexual de los menores).

---

[11] BENÍTEZ ORTUZAR IF. "Informática y delito"…, ob. cit., 114.

Así, puede afirmarse, sin riesgo de caer en error, que -en la mayoría de los casos- se considera que la sociedad tecnológica permite modalidades de conducta novedosas que afectan a bienes jurídicos tradicionales (intimidad y privacidad, propiedad, indemnidad sexual…), por lo que lo que se hace es modificar los tipos penales existentes describiendo conductas que incluyan las nuevas formas comisivas[12]. Las tecnologías de la información y la comunicación dan lugar a nuevas formas de realización de delitos tradicionales, que cada vez dificultan más su persecución. Al respecto, con el objetivo de mejorar y coordinar la lucha contra esta delincuencia informática o ciberdelincuencia, la Fiscalía General del Estado en la primera década del siglo XXI creaba un servicio específico de Criminalidad Informática[13].

Ahora bien, sobre todo para articular una investigación y persecución de estas conductas delictivas con unas mínimas garantías de éxito, ante la globalización que implica el uso de Internet y las tecnologías de la era informática con la irrupción del big data también en el mundo de la delincuencia, es necesario un consenso internacional que, de un lado, permita armonizar el Derecho penal sustantivo en la materia y, de otro lado, aporte instrumentos para agilizar la cooperación policial y judicial entre Estados. En esta línea, el mayor consenso existente sobre la "delincuencia informática" lo conforma el "Convenio sobre ciberdelincuencia" del Consejo de Europa" de 23 de noviembre de 2001[14] y un protocolo adicional al mismo de 2003 ("protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos"[15]).

En todo caso, el estudio sobre la cibercriminalidad en España de 2019, tomando datos del Sistema Estadístico de Criminalidad, sitúa la cibercriminalidad en un 9,9%, respecto del conjunto de la criminalidad en 2019, lo que supone una línea en constante crecimiento desde el año 2016, que se situaba en el 4,6%[16].

2. EL CONVENIO SOBRE CIBERDELINCUENCIA DEL CONSEJO DE EUROPA

En el seno del Consejo de Europa, con la participación además de Estados Unidos, Canadá, Sudáfrica y Japón, fruto del trabajo elaborado por un comité de expertos, tras

[12] Crítica con esta técnica de tipificación se muestra ÁLVAREZ VIZCAYA, M., "Consideraciones político criminales sobre la delincuencia informática: El Papel del Derecho penal en la red", Internet y Derecho penal, Cuadernos de Derecho Judicial, 10, Madrid 2001, páginas 257 y siguientes.

[13] Al respecto la Instrucción 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías.

[14] Ratificado por España en Instrumento de Ratificación de 20 de mayo de 2010 (BOE n. 226, de 17 de septiembre de 2010).

[15] Ratificado por España en Instrumento de Ratificación de 11 de noviembre de 2014 (BOE n. 26, de 30 de enero de 2015).

[16] Estudio sobre la cibercriminalidad… ob. cit., página 18.

veinticinco borradores, el 23 de noviembre de 2001, es firmado en Budapest el instrumento jurídico internacional que resulta ser el que presenta un mayor consenso en la lucha contra delincuencia desarrollada a través o por medio de la tecnología de la información y la comunicación. Se trata del Convenio sobre Ciberdelincuencia del Consejo de Europa, firmado en Budapest el 23 de noviembre de 2001, al que se han ido adhiriendo formal o informalmente Estados y organismos distintos del ámbito europeo, siendo reconocido en la práctica como la guía básica en la lucha contra la ciberdelincuencia a nivel internacional[17]. En este sentido, en el marco de la investigación y persecución del delito, la sexta conferencia internacional sobre ciberdelincuencia de la INTERPOL, celebrada en El Cairo, del 13 al 15 de abril de 2005, elaboraba una resolución en cuya primera recomendación se establecía expresamente "*que se utilice el Convenio sobre Ciberdelincuencia del Consejo de Europa como referencia en materia de normas internacionales procedimentales y legales mínimas para la lucha contra la ciberdelincuencia. Se instará a los países a suscribirlo. Este convenio se distribuirá a todos los países miembros de la INTERPOL en los cuatro idiomas oficiales*"[18].

El Convenio se estructura en un preámbulo y 48 artículos sistematizados en cuatro Capítulos, del modo siguiente: el Capítulo Primero (artículos 1) a la "terminología"[19]; el Capítulo Segundo (artículos 2 a 22) a las "medidas que deberán adoptarse a nivel nacional", subdividido a su vez en tres secciones, la primera dedicada al Derecho Penal Sustantivo (artículos 2 a 13)[20], la segunda al Derecho Procesal (artículos 14 a 21) y la tercera (artículo 22) a la Jurisdicción; el Capítulo Tercero (artículos 23 a 35) a la "cooperación internacional", subdividido a su vez en dos secciones, la primera relativa a los Principios generales[21] y la segunda a las disposiciones especiales[22]; el Capítulo Cuarto (artículos 36 a 48), a las "disposiciones finales"[23].

---

[17] Al respecto, vid. SÁNCHEZ BRAVO, A., "El Convenio del Consejo de Europa sobre Cibercrimen: Control vs. Libertades Públicas", La Ley, 2002-3, páginas 1851 y siguientes; MORALES GARCÍA, O., "Apuntes de política-criminal en el Convenio del Consejo de Europa sobre Cyber-crime", Delincuencia Informática. Problemas de Responsabilidad. Madrid 2002, páginas 13 y siguientes.

[18] 6ª. Conferencia Internacional sobre ciberdelincuencia. El cairo (Egipto), del 13 al a5 de abril de 2005, "La Cibercriminalidad: Un Desafío Global, Una Respuesta Universal".

[19] Determinando lo que se entiende, a efectos del Convenio, por "sistema informático", "datos informáticos", "proveedor de servicios" y "datos sobre el tráfico".

[20] "Disposiciones Comunes", "Conservación rápida de datos informáticos almacenados", "orden de presentación", "Registro y confiscación de datos informáticos almacenados", "Obtención en tiempo real de datos sobre el tráfico", "Interceptación de datos sobre el contenido".

[21] "Principios generales relativos a la cooperación internacional", "principios relativos a la extradición", "principios generales relativos a la asistencia mutua", "procedimientos relativos a las solicitudes de asistencia mutua de acuerdos internacionales aplicables".

[22] "Asistencia mutua en materia de medidas provisionales", "asistencia mutua en relación con los poderes de investigación", "Red 24/7".

[23] "Firma y entrada en vigor", "Adhesión al Convenio", "Aplicación territorial", "Efectos del Convenio", "Declaraciones", "Cláusula federal", "Reservas", "Enmiendas", "Solución de controversias", "Consulta entre las Partes", "Denuncia", "Notificación".

Tras dar una definición auténtica de lo que se entiende por "sistema informático"[24], "datos informáticos"[25], "proveedor de servicios"[26] y "datos sobre el tráfico"[27], en lo que se refiere a las medidas de Derecho penal sustantivo que deberán adoptarse a nivel nacional, clasifica los tipos penales en cuatro grupos de delitos:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos.
- Delitos informáticos.
- Delitos relacionados con el contenido.
- Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

Además, el Convenio sobre Ciberdelincuencia del Consejo de Europa recoge también la necesidad de que cada Estado en su Derecho Interno, adopte las medidas legislativas necesarias para castigar la participación con en la actividad delictiva de otro ("cualquier complicidad intencionada con vista a la comisión de alguno de los delitos previstos… con la intención de que se cometa ese delito") y la tentativa en este tipo de delitos ("cualquier tentativa de comisión de alguno de los delitos…cuando la tentativa sea intencionada"), dejando –no obstante– a la reserva de cada Estado la posibilidad de aplicar en todo o en parte el castigo de la tentativa de comisión de estos delitos[28].

Al mismo tiempo, sin perjuicio de la responsabilidad penal de la persona física que haya cometido el delito, también prevé la necesidad de establecer la responsabilidad directa de la persona jurídica, cuando sean cometidos por cuenta de las mismas por cualquier persona física. La responsabilidad de la persona jurídica podrá ser civil, penal o administrativa, de acuerdo con el tratamiento que dé el Derecho interno de cada Estado a la problemática relativa a la responsabilidad de estos entes por el hecho típico cometido[29].

---

[24] "Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa".

[25] "Cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función".

[26] "i. Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y ii. Cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio".

[27] Cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente".

[28] Artículo 11 del Convenio sobre Ciberdelincuencia del Consejo de Europa.

[29] Artículo 12 del Convenio sobre Ciberdelincuencia del Consejo de Europa; al respecto, vid. Silva Sánchez, J., "La responsabilidad penal de la persona jurídica en el Consejo de Europa sobre Ci-

Prevé la necesidad de establecer sanciones "efectivas, proporcionas y disuasorias, incluidas las penas privativas de libertad", para las personas físicas, y las "sanciones pecuniarias", para las personas jurídicas, consideradas responsables del delito[30].

Además, con posterioridad, el 30 de enero de 2003 en Estrasburgo se acuerda el "Protocolo adicional al Convenio sobre ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos". Este Protocolo adicional al Convenio sobre Ciberdelincuencia del Consejo de Europa, tiene la finalidad de completar el Convenio sobre Ciberdelincuencia por lo que respecta a la tipificación penal de los actos de índole racista y xenófoba cometidos mediante sistemas informáticos.

En este protocolo adicional, de 30 de enero de 2003, los Estados se comprometen a elaborar la legislación interna necesaria para perseguir y colaborar en la persecución de los delitos relativos a la Difusión de material racista y xenófobo mediante sistemas informáticos, las amenazas con motivación racista o xenófoba, los insultos con motivación racista o xenófoba, la negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad[31]. En el Código penal español este tipo de motivación en cualquier delito da lugar a la aplicación de la circunstancia agravante genérica del artículo 22.4 CP, consistente en la comisión del delito por "motivos racistas, antisemitas u otra clase de discriminación referente a la ideología, religión o creencias de la víctima, la etnia, raza o nación a la que pertenezca, su sexo u orientación sexual, razones de género, la enfermedad que padezca o su discapacidad"[32]. Por su parte, el artículo 510.3 CP, dentro de los delito relativos al ejercicio de los derechos fundamentales y libertades públicas y, más concretamente, en relación a los delitos cometidos con ocasión del ejercicio de los derechos fundamentales y de las libertades públicas garantizadas por la Constitución, incluye un tipo agravado respecto de las distintas modalidades de incitación a la violencia, discriminación, hostilidad y al odio, cuando se realicen "a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información".

3. DELITOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE DATOS Y SISTEMAS INFORMÁTICOS

El primero de los grupos de delitos que abarca el Convenio sobre Ciberdelincuencia del Consejo de Europa es el que afecta a la intimidad, en sus distintas manifestacio-

bercriminalidad", Delincuencia Informática. Problemas de Responsabilidad. Madrid 2002, páginas 113 y siguientes.

[30] Artículo 13 del Convenio sobre Ciberdelincuencia del Consejo de Europa.

[31] Al respecto, vid. PAVÓN PÉREZ, J.A., "La labor del Consejo de Europa en la lucha contra la cibercriminalidad: El protocolo adicional al Convenio sobre Cibercriminalidad relativo a la incriminación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos", Universidad de Extremadura. Anuario de la Facultad de Derecho, vol. XXI, 2003, páginas 187 y siguientes.

[32] En su redacción dada por Ley Orgánica 1/2015, de 30 de marzo.

nes, incluyendo el acceso y la interferencia en los datos de un sistema informático, la interferencia en el propio sistema informático con incidencia en los datos del propio sistema o el abuso de dispositivos que permitan las actividades anteriores. El espectro de conductas que se incluyen en este primer grupo de delitos es muy amplio, incluyendo la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos que incorporan estos datos. Los datos son aquellos que afectan tanto a la persona física como a la persona jurídica, incluyéndose en este apartado los delitos relativos al descubrimiento y revelación del secreto de empresa, por ejemplo.

En este grupo de delitos relativos a los sistemas de información, en el ámbito de la Unión Europea, fue absolutamente relevante, con incidencia directa en la legislación penal española, la Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques de los que son objeto los sistemas de información, la cual tenía por objeto "*reforzar la cooperación judicial en materia penal relativa a los ataques contra los sistemas de información mediante la instauración de instrumentos y procedimientos eficaces*". Esta Decisión Marco, además delimitaba terminológicamente el concepto de "sistema de información" y de "datos informáticos", en la línea en la que lo hace el Consejo de Europa en el Convenio sobre Ciberdelincuencia, además de dar una interpretación auténtica de lo que se debía considerar "sin autorización" y por "persona jurídica".

La Decisión Marco 2005/222, de 24 de febrero, fue sustituida por 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. La directiva, en su artículo primero establece las "normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información. También tiene por objeto facilitar la prevención de dichas in fracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes". El artículo 2 de la Directiva 2013/40/UE, incluyendo alguna precisión terminológica, prácticamente reproduce las definiciones de "sistema informático", "datos informáticos", "persona jurídica" y "sin autorización", ya recogidas en la sustituida Decisión Marco 2005/222, de 24 de febrero.

Al respecto, se entiende por "sistema informático"[33] "*todo aparato o grupo de aparatos interconectados o relacionados entre si, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático 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*".

Por su parte, se consideran "datos informáticos" [34] "*toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de*

[33] Vid nota n. 24.

[34] Vid nota n. 25.

información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función".

Considera además la Directiva que se entenderá "sin autorización" "*el acceso, la interferencia o la interceptación, que no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo o no permitido por el Derecho nacional*", *al tiempo que entiende por "persona jurídica" a "toda entidad a la cual el derecho vigente reconoce este estatuto, salvo los Estados y otros organismos públicos que ejercen prerrogativas públicas y las organizaciones internacionales de carácter público*"[35].

3.1. Acceso ilícito

El artículo 2 del Convenio sobre Ciberdelincuencia del Consejo de Europa establece que cada Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el "*acceso deliberado e ilegítimo a la totalidad o parte de un sistema informático*". Los Estados podrán exigir que se cometa infringiendo medidas de seguridad, con intención de obtener datos informáticos o con intención de cometer otra actividad delictiva[36].

Por su parte, en la misma línea, 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, en su artículo 3 obliga a los Estados miembros de la Unión Europea adoptar "*las medidas necesarias para que, cuando haya sido realizado intencionadamente, el acceso sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal cuando se haya cometido con violación de una medida de seguridad, al menos en los casos que no sean de menor gravedad*"[37].

Uniendo ambas redacciones, puede considerarse que el acceso ilegítimo y deliberado a todo o parte de un sistema de información es el acceso intencionado sin autorización. Ambos textos internacionales dejan a cada Estado la decisión de incluir en el ámbito del Derecho penal, atendiendo al principio de intervención mínima,

---

[35] Artículo 2, apartados d) y c), respectivamente, de la Directiva 2013/40/UE, del Parlamento Europeo y del Consejo, de 12 de agosto de 2013.

[36] Son múltiples las medidas de seguridad que se incorporan a un sistema informático para proteger los datos protegidos que pueden verse vulnerados. Por ejemplo, medidas de confidencialidad, autenticación, cifrado, firma digital, control de acceso…

[37] En la misma línea se pronunciaba la Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques de los que son objeto los sistemas de información, en su artículo 2, relativo al "acceso ilegal a los sistemas de información", señalaba que "cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad". Señalando igualmente que sólo sean objeto de acciones judiciales las infracciones que se comentan transgrediendo medidas de seguridad.

sólo las conductas más graves e intolerantes, es decir, el acceso con la finalidad de obtener datos informáticos o con la finalidad de cometer otra actividad delictiva. Si bien, la Directiva de la 2013/40/UE extiende dicho mandato a los casos en los que con el acceso intencionado se transgreden medidas de seguridad previamente existentes.

El "acceso ilícito" o ilegal a los medios de información, conocido como hacking, no aparecía recogido de modo expreso en el Código Penal español hasta la reforma operada por Ley Orgánica 5/2010, de 22 de junio. Hasta ese momento sólo era posible advertirlo de modo indirecto dentro de los delitos "contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio" en el artículo 197.2 CP, donde se incluye el tipo genérico consistente en quien, "*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*", *al igual que "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*"[38].

En relación a las obligaciones adquiridas por el Estado Español en relación a los textos internacionales vinculantes a los que se ha hecho referencia, se observa que el tipo genérico del artículo 197.2 CP exigía que el acceso ilícito a los sistemas informáticos -la utilización, apoderamiento o modificación- se realizara "en perjuicio de tercero"; requisito no exigido en los compromisos adquiridos, si bien, podría interpretarse como que cuando no existiera perjuicio de tercero, esos accesos se considerasen "de menor gravedad", atendiendo al principio de intervención mínima del Derecho penal.

No obstante, la Ley Orgánica 5/2010, de 22 de junio de reforma del Código penal incluyó un nuevo tipo penal, en el que se tipifica expresamente el acceso no autorizado a los sistemas informáticos, sin la exigencia en la conducta descrita que el hecho se realice en perjuicio de tercero. Así, se incluía un apartado 3 en el artículo 197 CP con la siguiente redacción: "*el que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera 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 legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años*". Optando por la línea políticocriminal más restrictiva, como modalidad delictiva desprovista de cualquier intención específica[39], que castiga cualquier acceso no autorizado a datos contenidos en un sistema informático, vulnerando las medidas de seguridad estable-

[38] Y en el caso de la tutela de los secretos de empresa en el artículo 278.1 CP, en tanto en cuanto remite a las modalidades comitivas del artículo 197 CP.

[39] Al respecto, vid. MORÓN LERMA, E., Internet y Derecho penal: "hacking", y otras conductas ilícitas en la red., Pamplona 2002, página 70.

cidas para impedirlo, al margen de la finalidad del acceso y del perjuicio causado al titular de los datos o a terceros. Al respecto consideró la doctrina que con este nuevo tipo penal es algo distinto a la "intimidad personal", que podría concretizarse en "la seguridad en el medio informático y la confidencialidad de la información que en él se contiene o por el que se transmite"[40].

Por su parte, la Ley Orgánica 1/2015, de 30 de marzo, incorpora un nuevo artículo 197bis. En el mismo traslada a su apartado primero el anterior artículo 197.3 CP, incorporando además la modalidad comisiva de "facilitar a otro" el acceso[41]. Por otra parte, cambia la redacción, pasando de exigir un "acceso a los datos o programas informáticos contenidos en un sistema informático o en parte del mismo" al "acceso al conjunto o parte de un sistema de información", abarcando un abanico de modalidades conductuales de mas amplio espectro[42].

Además, con una simple traslación del artículo 7 de la Directiva 2013/40UE, el legislador español adelanta el ámbito de intervención penal a momentos muy anteriores al de la materialización del acceso ilícito a los sistemas de información, incluyendo un nuevo artículo 197ter CP con la siguiente redacción: "*será castigado con la 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 los que se refieren los artículos 1 y 2 del artículo 197 o del artículo 197bis: 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*"[43].

Esta opción del legislador español implica en la práctica que todas las actividades de la llamada "comunidad Hackers", sin el consentimiento del titular de los datos o de los programas incluidos en el sistema informático cuyas medidas de seguridad se vulneran, entrarían dentro de esta figura delictiva, incluyendo las entradas no consentidas a sistemas o programas por simple curiosidad o para descubrir "agujeros de seguridad" que comunican a los titulares de los sistemas para que procedan a su reparación. Además, la inclusión del artículo 197ter CP supone la plasmación de un

---

[40] CARRASCO ANDRINO, M.M., "El delito de acceso ilícito a los sistemas informáticos", en Álvarez García/González Cussac (Dirs.), *Comentarios a la reforma penal de 2010*, Valencia 2010, página 250.

[41] Traslado que es considerado muy acertado, por tener un objetivo de tutela diferenciado de la intimidad personal del artículo 197 CP, por CASTELLÓ NICÁS, N., en "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio y delitos contra el honor", en Morillas Cueva (Dir.) *Estudios sobre el Código penal reformado (leyes orgánicas 1/2015 y 2/2015*), Madrid 2015, página 506.

[42] CASTELLÓ NICÁS, N., en "Delitos contra la intimidad…, ob. cit., página 507.

[43] En línea con el artículo 7 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013.

intervencionismo penal que puede llegar a los actos preparatorios de los actos preparatorios para el acceso ilícito a sistemas informáticos[44].

3.2. Interceptación ilícita

El artículo 3 del Convenio sobre Ciberdelincuencia del Consejo de Europa establece que cada Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno "*la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Pudiendo cada Estado exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático*".

En la misma línea, el artículo 6 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, exige a los Estados de la Unión Europea la "*adopción de medidas necesarias para garantizar que la interceptación, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionadamente y sin autorización, sea sancionable como infracción penal, al menos en los casos en los que no sean de menor gravedad*".

Tradicionalmente el "acceso ilícito" o "ilegal a los medios de información" aparecía recogido de forma genérica en el Código Penal español, dentro de los delitos "contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio" en el artículo 197.1 CP, donde se dispone lo siguiente: "*El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus……mensajes de correo electrónico... o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses*"[45].

---

[44] "Una suerte de actos preparatorios", los denomina SAINZ-CANTERO CAPARRÓS, J.E., en AA.VV. Morillas Cueva (dir.), Sistema de Derecho Penal. Parte Especial, Madrid 2020, página 359; también, CASTELLÓ NICÁS, N., en "Delitos contra la intimidad…, ob. cit., página 508.

[45] Al respecto, vid. ROMEO CASABONA, C.M., "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de la red", Revista Aranzadi de derecho y nuevas tecnologías, n. 10, 2006. Pamplona 2006, páginas 15 y siguientes, también "La protección penal de la intimidad y de los datos personales: los mensajes de correo electrónico y otras comunicacio-

El Código penal no especificaba en este caso ninguna referencia a "la interceptación ilícita de datos informáticos comunicados en transmisiones no públicas", sin embargo, la cláusula genérica de "cualquier otra señal de comunicación", permitía incluir perfectamente la referencia a la interceptación de datos comunicados en transmisiones efectuadas a través de un sistema informático.

Ahora bien, la Ley Orgánica 1/2015, de 30 de marzo, incluye un nuevo artículo 197 bis.2 CP, en el siguiente sentido: "*El que con 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 la pena de prisión de tres meses a dos años o multa de tres a doce meses*". El legislador español, en clave de un exacerbado expansionismo punitivo, incluye la tipificación expresa de la interceptación de datos informáticos (desde, hacia o dentro de un sistema de información), sin la exigencia de perjuicio de tercero, esto es, sin diferenciar la mayor o menor gravedad de la interceptación ilegal que le habilitaba la Directiva europea.

Además, la previsión de la tipificación expresa de los actos previos a los actos preparatorios del artículo 197ter CP, transcrito en el epígrafe anterior, también es aplicable a este tipo del artículo 197bis.2 CP, dándose la circunstancia -absurda- de que el tipo del artículo 197ter CP prevé una pena que en el intervalo mínimo de la pena privativa de libertad es superior al del articulo 197bis.2 CP, mientras que el intervalo de la pena alternativa de multa, en su límite superior es mayor el tipo de los actos preparatorios la interceptación que el de la propia interceptación consumada.

3.3. Interferencia en los datos

El artículo 4 del Convenio sobre Ciberdelincuencia del Consejo de Europa establece que cada Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno "*la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos*". Asimismo, en su Derecho interno, los Estados -para calificar estos actos como delito- podrán reservarse el Derecho a exigir que dichos actos "provoquen daños graves".

Por su parte, en la misma línea, el artículo 5 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[46], dispone lo siguiente: "*los Estados miembros adoptarán*

---

nes de carácter personal a través de Internet y problemas sobre la ley penal aplicable", Estudios Jurídicos. Ministerio Fiscal, n. 2, Madrid 2003, páginas 73 y siguientes.

[46] La sustituida Decisión Marco 2005/222/JAI, del Consejo, de 24 de febrero de 2005, relativa a los ataques de los que son objeto los sistemas de información, en su artículo 4, relativo a la "intromisión

las medidas necesarias para que borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles, datos informáticos contenidos en un sistema de información, intencionadamente y sin autorización, sea sancionable como infracción pena, al menos en los casos que no sean de menor gravedad".

La traslación de la Directiva 2013/40/UE al texto punitivo se realiza en el Capítulo IX, "de los daños", del Título XIII, "Delitos contra el patrimonio y contra el orden socioeconómico", del Libro segundo del Código penal.

Tras la redacción dada por la Ley Orgánica 1/2015, de 30 de marzo, en el artículo 264 CP, se castigan los daños en los sistemas informáticos; Dicho 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.*

---

ilegal en los datos" señalaba que cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad. En su artículo 6.2., señalaba la obligatoriedad de que cada Estado adopte las medidas necesarias para garantizar que "intromisión ilegal en los datos", sea castigada con sanciones penales de uno a tres años de prisión como mínimo en su grado máximo.

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.»

En el artículo 264.1 CP, se tipifica el tipo básico de daños informáticos, con la estructura del delito de daños comunes. La naturaleza del bien jurídico tutelado es discutible: por su ubicación, se trata de un delito patrimonial, por su contenido podría considerarse que se está más cerca de la protección de la indemnidad de los datos o de la propia seguridad informática. La doble exigencia de la gravedad en el borrado, daño, deterioro, alteración, supresión o inaccesibilidad al objeto material del delito, y a cuando el resultado producido sea grave, aún cuando no es la más correcta redacción de un tipo penal, debe ser interpretada en un sentido patrimonial, es decir, evaluable económicamente, aunque no requiera una expresa cuantificación para su consumación. Al respecto, la Sentencia de la Audiencia Provincial de Sevilla (sección séptima) n. 516/2011, de 30 de diciembre, afirma que "*no es infracción que precise de cuantificación económica para su apreciación. Lo que si exige el tipo penal que aplicamos es el daño causado sea grave*".

El objeto material del delito serán los elementos lógicos de un sistema informático, es decir, aquellos que no pueden ser leídos directamente por el. Al respecto, la Sentencia de la Audiencia Provincial de Valencia (sección cuarta) n. 447/2011, de 10 de junio, afirma que no se trata de dar respuesta, como hace el tipo básico ordinario del delito de daños del artículo 263 CP, a la "*afectación de un bien, de un objeto material perfectamente tangible, por lo era de fácil comprensión la idea de la destrucción, de rotura que este delito implica, frente al supuesto ahora valorado, en que estamos hablando de algo intangible, inmaterial como es un programa informático, que se hace más etéreo aun, cuando pensamos que estos se integran en una red, prácticamente ilimitado, que los intercomunica, que hace que una alteración puede que individualmente considerada no sea de una gran trascendencia, pero si esta se contempla tomando en consideración la totalidad de los usuarios afectados, sí que llega a tomar un verdadera trascendencia, generando unos importantes daños*".

La reforma operada por Ley Orgánica 1/2015, de 30 de marzo, en el tipo básico 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 inaccesibles, 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 trasposición de la directiva 2013/40/UE al derecho interno. Así el tipo castiga al que por cualquier medio o procedimiento y sin estar autorizado de manera grave borre, deteriore, altere suprime o hace inaccesibles los datos informáticos, los programas informáticos o cualquier documento

electrónico ajeno y provoque un resultado grave en los mismos; es decir, en principio y salvo lo que más adelante se apunta respecto de la nueva modalidad agravada del artículo 264.2.5ª CP, cualquier conducta que por medios físicos o por medios lógicos los destruya o inutilice, en tanto que se trata de un delito de resultado, en el que cabe la tentativa. El resultado dañoso se refiere a la causación de un daño funcional de los elementos lógicos objeto del delito.

El tipo, por otra parte, mantiene la discutible y controvertida reiteración de la gravedad típica: de la gravedad del hecho y del resultado sobre los elementos lógicos, es decir, sobre aquellos elementos que no pueden ser leídos o percibidos directamente por el hombre[47].

Al respecto, la Circular 3/2017 de la Fiscalía General del Estado, sobre la reforma del Código Penal operada por L.O. 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los daños informáticos (en adelante Circular 3/2017 de la Fiscalía General del Estado), afirma que "*habría que considerar graves, y por tanto, encuadrables por su resultado en el art. 264.1 CP, todas aquellas acciones ilícitas que tuvieran trascendencia significativa o generaran consecuencias apreciables en datos, programas informáticos o documentos electrónicos o en los intereses en juego*". En esta línea, la Sentencia de la Audiencia Provincial de Jaén (sección segunda) n. 25/2018, 6 de febrero, dispone lo siguiente: "*surge así un problema de interpretación sobre el concepto de <<daño grave>>, ya que el legislador no proporciona criterios que aclaren la cuestión. Como se señala en las Sentencias de la AP Madrid 10/1/2017, AP Barcelona 26/2018, o AP Palencia 14/7/2016, no parece que el resultado grave deba ser identificado con una valoración del mismo superior a 400 € que permita distinguir el delito menos grave del delito leve, pues no existe una tipificación de esta figura penal como delito leve. El resultado grave de los daños causados en los delitos informáticos deberá ser estimado caso por caso atendiendo a criterios que permitan apreciar esa gravedad, criterios como puede ser la posibilidad o no de recuperar los datos informáticos, la perdida definitiva de los mismos o la posibilidad de recuperación y, en éste último caso, el coste económico de la reparación del daño causado, la complejidad técnica de los trabajos de recuperación, la duración de las tareas de recuperación, el valor del perjuicio económico causado al titular de los datos, bien como lucro cesante o como daño emergente*".

Por otra parte, el artículo 264.2 CP CP incluye cinco circunstancias que fundamentan un tipo agravado del delito de daños informáticos:

— El artículo 264.2.1ºCP, mantiene la circunstancia que fundamenta el tipo agravado de daños informáticos en el hecho de que se comentan en el marco de una organización criminal. A diferencia de otros delitos patrimoniales

[47] GONZALEZ RUS, J.J., en Morillas Cueva (Dir.) *Sistema de Derecho Penal Español. Parte Especial*, Madrid 2011, página 553.

(por ejemplo la circunstancia del artículo 235.1.9º CP) se refiere sólo a la organización criminal y no al grupo criminal, por lo que para aplicar el tipo agravado deberán de ejecutarse los hechos en el seno de una organización de dos o más personas con una estructura estable en la que de manera coordinada y concertada se repartan tareas y funciones con el fin de cometer el delito (artículo 570bis CP).

— El artículo 264.2.2º CP, incluye una modalidad agravada atendiendo a la gravedad del resultado producido: que "*haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos*". Centrando, de este modo, la triple gravedad de la magnitud del daño originado, en la especial gravedad del daño o en el número de sistemas afectado. Junto a la gravedad de la acción y la gravedad del resultado del tipo básico, para aplicar este tipo agravado deberá producirse esta triple agravación (especial gravedad de los daños o la afectación a un número elevado de sistemas informáticos).

  Dicha gravedad se proyecta de forma alternativa en el tipo, bastando para su aplicación que concurran daños de "especial gravedad" o que afecten "a un número elevado de sistemas informáticos". La especial gravedad de los daños aparece de forma indeterminada y de difícil concreción, impropia de la redacción del tipo penal. Por lo que respecta al numero elevado de sistemas informáticos que deben verse afectados, la Circular 3/2017 de la Fiscalía General del Estado, sobre la reforma del Código Penal operada por L.O. 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los daños informáticos, lo equipara a la existencia de un "ataque informático masivo". Al respecto, la Sentencia de conformidad de la Audiencia Nacional n. 17/2015, de 11 de junio, aplica este tipo agravado a unos hechos consistentes en dañar programas informáticos o documentos electrónicos ajenos mediante la propagación de un virus o código malicioso infectando a 23.662 ordenadores "para crear una red zombi".

— 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*". Esta modalidad agravada también exige una triple gravedad: gravedad en el hecho, gravedad en el resultado lesivo a los sistemas informáticos y que afecte gravemente al funcionamiento de los servicios esenciales o a la provisión de bienes de primera necesidad. También aparece de forma alternativa, es decir, será aplicable cuando perjudique gravemente el funcionamiento de los servicios públicos esenciales, por un lado, o, por otro lado, cuando perjudique gravemente la provisión de bienes de primera necesidad.

El tipo no define qué servicios esenciales son los que deben verse afectados. Al respecto, Circular 3/2017 de la Fiscalía General del Estado afirma que "*a estos efectos se entienden por servicios esenciales aquellas actividades que sirven para el funcionamiento de las funciones sociales básicas de la comunidad, como la salud, la seguridad, la protección de los derechos fundamentales y las libertades públicas y el normal funcionamiento de las Instituciones del Estado*". No obstante, deberán excluirse aquellos daños que afecten a servicios públicos esenciales calificados como de infraestructuras críticas o que afecten a la seguridad del Estado, de la Unión Europea o de un Estado miembro de la Unión Europea, en cuyo caso será de aplicación preferente el tipo del apartado 4º del mismo artículo 264.2 CP[48].

Respecto a la gravedad en el sistema informático que afecte gravemente a la provisión de bienes de primera necesidad, Señala la Circular 3/2017 de la Fiscalía General del Estado que "*deberán considerarse como tales los alimentos, medicamentos y otros productos de consumo imprescindible para la subsistencia y la salud de las personas*". Su gravedad específica aparece también indeterminada, debiendo dotarse de contenido jurisprudencialmente[49].

— 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*". *Señalando expresamente lo que, a* estos efectos, se considera infraestructura crítica, es decir, "*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*".

También esta modalidad agravada aparece tipificada de forma mixta alternativa. Por un lado será aplicable cuando los daños afecten al servicio informático de una infraestructura crítica, y, por otro lado, *también cuando con ellos 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*.

En el primer inciso la triple gravedad del hecho se fundamenta en la mera afectación a la infraestructura crítica, lo cual ya es en sí mismo un resultado grave. En este sentido también la Circular 3/2017 de la Fiscalía General del Estado.

[48] BENÍTEZ ORTUZAR, I.F. en "De los daños", en Morillas Cueva (Dir.) *Estudios sobre el Código penal reformado (leyes orgánicas 1/2015 y 2/2015*), Madrid 2015, página 605.

[49] BENÍTEZ ORTUZAR, I.F. en "De los daños"…, ob. cit., página 605.

Sin embargo, para la segunda modalidad de conducta alternativa, exige que los daños informáticos generen una grave situación de peligro para la seguridad del Estado de la Unión Europea o de algún Estado de la Unión Europea. En este último caso, el tipo sigue siendo de resultado, en tanto que es necesario un grave perjuicio en los sistemas informáticos, pero que este daño informático ponga en situación de peligro la seguridad del Estado, de la Unión Europea o de otro Estado de la Unión Europea[50]; también la Circular 3/2017 de la Fiscalía General del Estado). Se trata de un delito pluriofensivo, en tanto que, además del elemento patrimonial lesionado se exige la puesta en peligro de la seguridad del Estado, de la Unión Europea o de un Estado miembro de la Unión Europea.

— 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. Esta modalidad típica es distorsionadora y no mantiene una coherencia con las cuatro restantes, en tanto que, no se agrava por la entidad cuantitativa o cualitativa del perjuicio causado. Por otra parte, puede dar lugar a la ruptura interpretativa, en tanto que cuando se accede a los datos informáticos, archivos informáticos o documentos electrónicos que se pretenden dañar o inutilizar a través de elementos lógicos, mediante claves de ordenador, código de acceso o claves similares, siempre sería de aplicación el tipo agravado: dejando, de este modo, el tipo básico exclusivamente para las destrucciones físicas de los datos informáticos, de los archivos informáticos o los documentos electrónicos.

  Respecto de la pena, se prevé una pena de dos a cinco años de prisión y multa del tanto al décuplo del perjuicio ocasionado (lo que supone un importante incremento punitivo respecto de la pena prevista para las modalidades agravadas en el artículo 264.3 CP anterior, que aparecía con el límite máximo de tres años de prisión y multa del tanto al décuplo del perjuicio ocasionado). Además, atendiendo al nuevo párrafo segundo del artículo 264.2 CP, en estos casos, la pena podrá ser la superior en grado en el caso en que el resultado de los daños producidos fuese de extrema gravedad (pudiendo llegar, por tanto, a los siete años y seis meses de prisión). El incremento punitivo, en este caso, es extremo, pasando de un máximo de tres años de prisión que se establecía con anterioridad a la reforma de 2015, a un máximo de siete años y seis meses de prisión, superando con creces lo exigido por la Directiva 2013/40/UE[51].

---

50 BENÍTEZ ORTUZAR, I.F. en "De los daños"…, ob. cit., página 606.

51 BENÍTEZ ORTUZAR, I.F. en "De los daños"…, ob. cit., página 610.

Por último, el artículo 264.3 CP recoge una agravación aplicable tanto al tipo básico, como a los tipos agravados, atendiendo a la forma de comisión del hecho, *"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*". Agravación que parece funcionar exclusivamente para las destrucciones o inutilizaciones "lógicas" de los elementos "lógicos", excluyendo las destrucciones físicas que no exigen el acceso a "lógico" a los sistemas informáticos.

La referencia a la "utilización ilícita" es compleja, en tanto que no señala qué se considera por actividad ilícita. Es posible que el titular de los datos de otra persona no tenga competencia para autorizar la utilización de sus datos, por ejemplo, para acceder a los sistemas informáticos de una infraestructura crítica, pero que el sujeto que accede de este modo los haya utilizado porque éste se los ha cedido, en cuyo caso el titular de los datos con los que se accede podría ser un cooperador necesario. Las posibilidades que respecto de las formas de participación en el mismo, unido a la agravación del artículo 264.2.5ª CP en relación con el artículo 264 ter CP son enormes. El tipo no exige, como sin embargo, planteaba la Directiva 2013/40/UE, la causación de daños al propietario legítimo de la identidad, al margen de que el acceso ilícito a los datos personales que se hallen registrados en ficheros o sistemas informáticos electrónicos o telemáticos ya se encuentran tipificados en el artículo 197.2 CP[52].

En línea con lo dispuesto en el artículo 7 de la la Directiva 2013/40/UE, del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, a Ley Orgánica 1/2015, de 30 de marzo, añadió 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 197ter CP, respecto de los delitos "*del descubrimiento y revelación de secretos*", al que nos remitimos.

---

[52] BENÍTEZ ORTUZAR, I.F. en "De los daños"…, ob. cit., página 607.

3.4. Interferencia en el sistema

El artículo 5 del Convenio sobre Ciberdelincuencia del Consejo de Europa establece que cada Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno "*la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos*".

Por su parte, el artículo 4 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[53], dispone lo siguiente: "*Los Estados miembros adoptarán las medidas necesarias para que las obstaculización o la interrupción significativas del funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, intencionalmente y sin autorización, como infracción penal, al menos en los casos que no sean de menor gravedad*"[54].

La Ley Orgánica 1/2015, de 30 de marzo, en sustitución del 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 informático ajeno:*
>
> *a) realizando alguna de las conductas a que se refiere el artículo anterior;*
>
> *b) introduciendo o transmitiendo datos; o*

---

[53] La sustituida Decisión Marco 2005/222/JAI, del Consejo, de 24 de febrero de 2005, relativa a los ataques de los que son objeto los sistemas de información, en su artículo 4, relativo a la "intromisión ilegal en los datos" señalaba que cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad. En su artículo 6.2., señalaba la obligatoriedad de que cada Estado adopte las medidas necesarias para garantizar que "intromisión ilegal en los datos", sea castigada con sanciones penales de uno a tres años de prisión como mínimo en su grado máximo.

[54] La sustituida Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques de los que son objeto los sistemas de información, en su artículo 4, relativo a la "intromisión ilegal en los datos" señala que cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad. En su artículo 6.2 señala la Decisión Marco citada, la obligatoriedad de que Cada Estado adopte las medidas necesarias para garantizar que "intromisión ilegal en los sistemas de información", sea castigada con sanciones penales de uno a tres años de prisión como mínimo en su grado máximo.

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.».

La sistematización de estos delitos de obstaculización o interrupción de los sistemas informáticos, al igual que en el caso de los daños informáticos del artículo 264 CP, se estructura en un tipo básico (artículo 264 bis.1 CP), un tipo agravado (artículo 264 bis.2 CP) y unas agravaciones específicas (artículo 264 bis.3 CP). 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. Al respecto, Circular 3/2017 de la Fiscalía General del Estado afirma que "*serían típicas aquellas acciones que se realizan intencionadamente sobre los mismos, con los objetivos indicados, sin estar habilitado para ello*".

La conducta exige que la obstaculización o la interrupción sea grave, sin llegar a que 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.

— 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.

— 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[55].

— 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.

En cuando a la modalidad de acceso a los datos informáticos objeto de estos delitos, la Sentencia de la Audiencia Provincial de Madrid (sección sexta) de 3 de junio de 2013, considera que, respecto de la conducta "*consistente en impedir, negando la clave de acceso, que se pudiera tener acceso en el ordenador*" donde se encuentran los datos que el acusado había borrado intencionadamente, se produce un concurso de normas con el delito de coacciones, y, *"en virtud de lo establecido en el art. 8 del Código Penal, apartado tercero, según el cual cuando los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de dicho Código, el precepto penal más amplio o complejo absorberá a los que castiguen las infracciones consumidas en aquel, tal concurso ha de resolverse en favor del delito de daños informáticos, que, por el mayor desvalor respecto al delito de coacciones absorbe la total antijuridicidad del hecho, por lo que debe quedar éste absorbido por aquel, por aplicación del principio de consunción*".

[55] BENÍTEZ ORTUZAR, I.F. en "De los daños"…, ob. cit., página 608.

3.5. Abuso de dispositivos

El artículo 2 del Convenio sobre Ciberdelincuencia del Consejo de Europa establece que cada Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la producción, venta, obtención para su utilización, importación difusión u otra forma de puesta a disposición de: a. un dispositivo, incluido en un programa informático, diseñado o adaptado principalmente para la comisión de los delitos anteriores; b. una contraseña, código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a parte de un sistema informático; y la Posesión de alguno de los elementos a. y b. del punto anterior con finalidad de cometer alguno de los delitos de este bloque. Pudiendo los Estados un número determinado de dichos elementos para exigir responsabilidad penal. Queda al arbitrio de cada Estado no castigar la producción y la posesión de estos dispositivos; Queda fuera cuando la conducta no tiene la finalidad de cometer un delito (para pruebas autorizadas o para protección de un sistema informático).

El artículo 7 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, bajo la rúbrica "Instrumentos utilizados para cometer las infracciones", indica que: "*los Estados miembros adoptarán las medidas necesarias para garantizar que la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de los siguientes instrumentos, sin autorización y con la intención de que sean utilizados con el fin de cometer cualquiera de las infracciones mencionadas en los artículos 3 a 6, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad: a) un programa informático, concebido o adaptado principalmente para cometer una infracción de las mencionadas en los artículos 3 a 6; 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*".

Con carácter previo a la ratificación por España del Convenio de Budapest y a la Directiva 2013/40/UE, esta tipología de conducta fue incluida en el Código penal por la Ley Orgánica 15/2003, de 25 de noviembre, en diferentes capítulos del texto punitivo: así, por ejemplo, en el artículo 248.2.b) CP (para las llamadas estafas informáticas)[56]; en el artículo 286 CP (para permitir el acceso no autorizado a

[56] Artículo 248.2.b) CP: "*También se consideran reos de estafa:... b) los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo*". En su redacción dada por Ley Orgánica 5/2010, de 22 de junio (tipo introducido en el Código penal por Ley Orgánica 15/2003, de 25 de noviembre).

servicios de acceso condicional o a equipos de telecomunicación)[57]; en el artículo 270.6 CP (delitos relativos a la propiedad intelectual)[58]; o en el artículo 400 CP, (de las falsedades)[59].

Ahora bien, es la Ley Orgánica 1/2015, de 1 de marzo, la que implementa en el Código Penal el mandato del artículo 7 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, incluyendo los artículos 197ter y 264ter CP, a los que se ha hecho referencia en apartados anteriores.

4. DELITOS INFORMÁTICOS

Como se afirmaba en epígrafes anteriores, el Convenio sobre Ciberdelincuencia, hecho en Budapest, el 23 de noviembre de 2001, tras a los "delitos contra la confiden-

---

[57] Artículo 286 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:*

1. 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.

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

2. 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.

3. A quien, 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.

4. 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". Introducido por Ley Orgánica 15/2003, de 25 de noviembre.

[58] Artículo 270.6 CP: "*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 tenga 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*". En su redacción dada por Ley Orgánica 1/2015, de 30 de marzo (tipo introducido en el Código penal por Ley Orgánica 15/2003, de 25 de noviembre).

[59] Artículo 400 CP "*la fabricación, recepción, obtención o tenencia de útiles, materiales, instrumentos, sustancias, datos, programas informáticos, aparatos, elementos de seguridad, u otros medios específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigará con la pena señalada en cada caso para los autores*".

cialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"[60], incluye un apartado específico dedicado a los "delitos informáticos" (artículo 7), entre los que incluye la "falsificación informática" y el "fraude informático" (artículo 8).

4.1. Falsificación informática

El artículo 7 del Convenio sobre Ciberdelincuencia del Consejo de Europa establece que cada Estado adoptará las medidas legislativas y de otro tipo para tipificar como delito la comisión de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que de lugar a datos no auténticos, con la intención de que sean utilizados a efectos legales como auténticos, con independencia de que los datos sean o no directamente legibles o ilegibles. Los Estados podrán exigir una intención fraudulenta o delictiva similar para exigir la responsabilidad criminal.

En el Código penal español este tipo de conductas constitutivas de la introducción, alteración, borrado o supresión de datos informáticos, dando lugar a datos no auténticos, con la intención de que sean utilizados como auténticos entra dentro de las figuras típicas de las falsedades documentales de los artículos 390 a 399 CP. La falsedad documental en el Código penal, sea en documento público o privado, realizada por funcionario público o particular, supone la alteración de un documento en alguno de sus requisitos o elementos de carácter esencial. La consideración de documento del sistema informático que tiene incorporados datos informáticos de las personas es posible atendiendo a la definición de documento que da el artículo 26 CP, que considera documento "*todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica*". De forma que, considerando el sistema informático que incorpora datos como soporte material, la alteración, modificación, introducción o borrado o supresión de estos datos con la intención de usar los resultantes como auténticos, da lugar a la comisión de la correspondiente figura delictiva relativa a las falsedades documentales[61].

---

[60] Concordante con 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.

[61] Al respecto, en este sentido, expresamente, SANCHÍS CRESPO, C., "La prueba por soportes informáticos (una perspectiva civil y penal)", Incorporación de las nuevas tecnologías al comercio: aspectos legales, Estudios de Derecho Judicial 71, Madrid 2006, página 327; FERNÁNDEZ PANTOJA, P., "Comentario al artículo 26", Comentarios al Código Penal, Tomo III, Madrid 2000, páginas 311-312; ORT BERENGUER, E./ROIG TORRES, M., "Delitos contra la intimidad, utilización fraudulenta de tarjetas de crédito y falsedad en documentos electrónicos", Incorporación de las nuevas tecnologías al comercio: aspectos legales, Estudios de Derecho Judicial 71, Madrid 2006, página 119-120; Bacigalupo Zapater, E., "Documentos electrónicos y delitos de falsedad documental", Delincuencia Informática. Problemas de responsabilidad, Cuadernos de Derecho Judicial 9, Madrid 2002, páginas 281 y siguientes; Mir Puig, C., "Sobre algunas cuestiones relevantes del Derecho Penal en Internet", Internet y Derecho penal, Cuadernos de Derecho Judicial, 10, Madrid 2001, páginas 283 y siguientes; DE URBANO CASTRILLO, E., "El documento electrónico: Aspectos procesales". Internet y Derecho penal, Cuadernos de

En todo caso, la Ley Orgánica 1/2015, de 30 de marzo, da una redacción al artículo 400 CP, adaptada a la exigencia del Convenio de Budapest sobre ciberdelincuencia, con la siguiente redacción: "*la fabricación, recepción, obtención o tenencia de útiles, materiales, instrumentos, sustancias, datos, programas informáticos, aparatos, elementos de seguridad, u otros medios específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigará con la pena señalada en cada caso para los autores*". Cláusula que vuelve a suponer un adelanto punitivo a actos preparatorios para la posterior comisión de la falsedad, que, como máximo, ponen en peligro el bien jurídico por sí solos, lo que es sumamente discutible[62].

4.2. Fraudes informáticos

El artículo 8 del Convenio sobre ciberdelincuencia obliga a las partes a adoptar en su Derecho interno las medidas legislativas y de otra índole dirigidas a tipificar como delito los actos deliberados e ilegítimos que causen perjuicio patrimonial a otras personas mediante: cualquier introducción, alteración, borrado o supresión de datos informáticos, o con cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio para sí o para un tercero.

Por su parte en el Derecho interno, el artículo 248.2 CP recoge lo que pueden denominarse "estafas impropias" en tanto se señala que "también se consideran estafas" una serie de conductas fraudulentas que si bien tienen en común con la estafa afectar de forma fraudulenta al patrimonio ajeno, se diferencia de ésta en la dinámica comisiva, en tanto que pierden lo más característico de la estafa que es su aspecto criminológico, que la convierte en un delito de encuentro en el que es imprescindible la participación de una víctima colaboradora. En estas estafas impropias no se produce un encuentro entre sujetos activo y pasivo ni se requiere, por tanto, una víctima colaboradora.

En estas estafas impropias se incluyen: a) La estafa cometida mediante manipulación informática; b) Conductas relacionadas con los medios informáticos aptos para cometer estafas, que conformarían más bien actos preparatorios de las estafas cometidas mediante manipulación informática; c) La utilización fraudulenta de tarjetas de crédito o débito o de cheques de viaje[63].

Derecho Judicial, 10, Madrid 2001, páginas 568 y siguientes; ROVIRA DEL CASTILLO, E., "Tratamiento penal sustantivo de la falsificación informática", Internet y Derecho penal, Cuadernos de Derecho Judicial, 10, Madrid 2001, páginas 576 y siguientes.

[62] MORILLAS CUEVA, L., en AA.VV. Morillas Cueva (dir.), Sistema de Derecho Penal. Parte Especial, Madrid 2020, página 1197.

[63] Al respecto, vid. BENÍTEZ ORTÚZAR, I.F, en AA.VV. Morillas Cueva (dir.), Sistema de Derecho Penal. Parte Especial, Madrid 2020, páginas 563 y siguientes.

4.2.1. Estafas por procedimientos informáticos

El artículo 248.2.a) CP: dispone que también se consideran reos de estafa: *"los que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una trasferencia no consentida de cualquier activo patrimonial en perjuicio de otro"*.

El tipo fue introducido de nuevo cuño por el Código penal de 1995. Con esta "sui géneris" modalidad de estafa se vino a colmar una laguna de punibilidad y a hacer frente a determinados ataques contra el patrimonio que, en puridad, no cumplen con todos los elementos de la estafa. En particular, falta el elemento esencial del delito de estafa: el "engaño a otra persona". Así la Sentencia del Tribunal Supremo de 19 de abril de 1991, antes de la entrada en vigor del Código penal de 1995, negó la calificación de estafa al supuesto en el que "*un apoderado de una entidad financiera que mediante alteraciones contables a través del ordenador, consigue la transferencia y ulterior apropiación de determinadas sumas de dinero de los clientes de la entidad*", por considerar que no existió el engaño a otra persona exigido en el delito de estafa, en tanto que, en realidad, se actuaba sobre una máquina.

El delito consiste en la introducción de órdenes falsas o ejecutar alteraciones en los programas que gestionan automáticamente transferencias bancarias, ingresos o reconocimiento de créditos a favor de quien realiza la manipulación (eficaz en los fraudes realizados mediante la banca electrónica y otros mecanismos de comercio electrónico).

Con este precepto se trata de criminalizar conductas lesivas para el patrimonio ajeno que, aún manteniendo una esencia fraudulenta, quedan al margen de la dinámica comisiva de la estafa propia.

La formulación es análoga a la estafa: cualquier modalidad comisiva ("alguna manipulación informática o artificio semejante") con un resultado lesivo a un activo patrimonial ajeno en perjuicio de tercero. Al respecto, la Sentencia del Tribunal Supremo n. 692/2006, de 26 de junio, señalaba lo siguiente: "*Como en la estafa debe existir un ánimo de lucro; debe existir la manipulación informática o artificio semejante que es la modalidad comisiva mediante la que torticeramente se hace que la máquina actúe; y también un acto de disposición económica en perjuicio de tercero que se concreta en una transferencia no consentida. Subsiste la defraudación y el engaño, propio de la relación personal, es sustituido como medio comisivo defraudatorio por la manipulación informática o artificio semejante en el que lo relevante es que la máquina, informática o mecánica, actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos, de aquellos que permite su programación, o por la introducción de datos falsos. Cuando la conducta que desapodera a otro de forma no consentida de su patrimonio se realiza mediante manipulaciones del sistema infor-*

mático, bien del equipo, bien del programa, se incurre en la tipicidad del art. 248.2 del Código Penal. También cuando se emplea un artificio semejante. Una de las acepciones del término artificio hace que éste signifique artimaña, doblez, enredo o truco".

Estas conductas no podían ser consideradas hurtos, por no suponer una sustracción propiamente dicha, no se trata de moneda escritural ni de cambio, realmente es una transferencia virtual de una cuenta a otra. Tampoco podían considerarse estafas por no existir engaño a otro. Sí se ha dicho que la estafa es una de las modalidades delictivas en las que la relación víctima-victimario es más peculiar, en esta modalidad no existe esta relación, ni hay engaño, ni se crea en otro una falsa representación de la realidad.

Se trata de una transferencia de un activo patrimonial en sentido contable. En eso se asemeja a la estafa, si bien, "virtual". No obstante, esta "virtualidad" rompe con el propio concepto de estafa al no existir la relación de causalidad engaño-error-acto de disposición.

En realidad en estos casos no existe una auténtica estafa pues no se engaña a una persona para que realice un acto de disposición patrimonial aunque sí existe un cierto fraude para lograr un enriquecimiento a costa de otro. Constituiría este delito, por ejemplo, la conducta del hacker que se introduce mediante su ordenador en el de un banco y ordena una transferencia a su cuenta o consigue modificar el programa de dicho banco para que se transfieran los decimales de todas las operaciones que se realicen en él a una determinada cuenta a su nombre.

La utilización fraudulenta de la tarjeta de crédito, no obstante, en principio no da lugar a esta modalidad delictiva, en tanto que se ha incorporado como modalidad específica de estafa impropia en el artículo 248.2.c) CP, por Ley Orgánica 5/2010, de 22 de junio.

4.2.2. Conductas relacionadas con los medios informáticos aptos para cometer estafas

La Ley Orgánica 15/2003, de 25 de noviembre, incluyó el actual artículo 248.2.b) CP, que, tras la reforma operada por Ley Orgánica 5/2010, de 22 de junio, aparece con la siguiente redacción: También se considerarán reos de estafa *"los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo*".

El legislador, en el afán expansionista de criminalizarlo todo, equipara a la estafa una descripción típica abierta y amplísima, que a diferencia de la estafa propia y la estafa informática, no requiere resultado patrimonial alguno.

En este tipo se castigan conductas relacionadas con programas informáticos concebidos con finalidades exclusivamente defraudatorias, elevándose a la cate-

goría de delito autónomo unos simples actos preparatorios de estafas, dirigidos a realizar alguno de los tipos de estafa propia, informática o relativos a las tarjetas de crédito o débito o cheques de viajes, en tanto que se refiere a las "estafas previstas en este artículo" 248 CP. Se anticipa el momento de la intervención penal por la preocupación que muestra el legislador en relación con las conductas llevadas a cabo con programas informáticos ya que son un instrumento de gran potencial lesivo tanto por el número de personas que pueden verse afectadas como por el volumen económico que puede alcanzar la defraudación.

En cuanto a las conductas descritas, abarcan un abanico muy amplio que iría desde simples actos preparatorios de la estafa común del artículo 248.1 CP o de la estafa informática del artículo 248.2.a) CP a conductas de participación (cooperación necesaria o complicidad, dependiendo del grado de participación) en la estafa informática o común de otros; donde también se incluye la incriminación de meras sospechas de futuras estafas (es muy peligroso especialmente el castigo de la simple posesión de este tipo de programas que fueron especialmente diseñados para realizar estafas), o de programas informáticos tendentes a facilitar las conductas fraudulentas llevadas a cabo con tarjetas de crédito del artículo 248.2.c) CP. De los trámites parlamentarios del proyecto de Ley que dio lugar a la Ley Orgánica 15/2003, de 25 de noviembre, no se extrae ninguna aclaración al no existir enmiendas al respecto.

Por ejemplo, será constitutivo de esta modalidad de estafa impropia la fabricación o posesión de un programa que sirve para la generación aleatoria de números válidos de tarjetas de crédito.

La conducta típica se concreta en la fabricación, introducción, posesión o facilitación de estos programas informáticos destinados específicamente a la comisión de estas estafas. El legislador no ha cambiado la fórmula "programas informáticos destinados específicamente a la comisión de estas estafas", por "programas informáticos concebidos o adaptados principalmente para la comisión de estas estafas", tal y como ha hecho, por ejemplo, en la Ley Orgánica 1/2015, de 30 de marzo, respecto de los programas informáticos utilizados para causar los daños en los sistemas informáticos en el artículo 264 ter. a). En todo caso, la aptitud para producir el perjuicio típico debe residir en el propio programa informático, no en la pericia del sujeto que lo utiliza.

4.2.3. La utilización fraudulenta de tarjetas de crédito o débito o cheques de viaje

La Ley Orgánica 5/2010, de 22 de junio, introdujo el artículo 248.2.c) CP, por el que también se consideran reos de estafa: *"los que utilizando tarjetas de crédito o débito, o datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero"*.

Se "consideraba estafa" de este modo, por disposición legal toda utilización fraudulenta de tarjetas ajenas o de los datos obrantes en ellas. Así se recogía en el preámbulo de la Ley Orgánica 5/2010, de 22 de junio: *"Entre las estafas descritas en el artículo 248 del Código Penal, cuyo catálogo en su momento ya se había acrecentado con los fraudes informáticos, ha sido preciso incorporar la cada vez más extendida modalidad consistente en defraudar utilizando las tarjetas ajenas o los datos obrantes en ellas, realizando con ello operaciones de cualquier clase en perjuicio de su titular o de un tercero*".

Hasta la entrada en vigor de este nuevo artículo 248.2.c) CP, estos atentados al patrimonio ajeno no quedaban impunes. Al respecto se solían distinguir varias hipótesis que en la actualidad deben ser consideradas estafas al establecer este precepto "la utilización de tarjetas de crédito o débito o cheques de viaje" directamente, o "los datos obrantes en cualquiera de ellos" (en operaciones por internet, por ejemplo), realizando "operaciones de cualquier clase", en perjuicio de su titular o de un tercero. Así la Jurisprudencia había realizado el siguiente esquema:

A. Utilización de tarjeta de crédito sustraída o extraviada en cajero: La Sentencia el Tribunal Supremo n. 427/1999, de 16 de marzo, consideraba el hecho robo con fuerza en las cosas en su modalidad de llaves falsas, equiparando el uso de la tarjeta magnética como llave falsa del artículo 239 CP): "*Con relación al nuevo 248.2… hay que entender que dicho fraude informático no contempla la sustracción de dinero a través de la utilización no autorizada de tarjetas magnéticas sobre los denominados <<cajeros automáticos>>, porque la dinámica comisiva no aparece alejada de la clásica de apoderamiento, aunque presenta la peculiaridad de la exigencia del uso de la tarjeta magnética para poder acceder al material del delito. Constituye así este supuesto una mera sustracción de dinero mediante la utilización por un tercero del específico medio de acceso del propietario del mismo, pero no alcanza a la conducta igualmente delictiva de transferencia de activos patrimoniales mediante la manipulación informática. No supone por ello el uso de la tarjeta por el no titular la <<manipulación informática>> o artificio semejante que requiere el precepto, al no concurrir en supuestos de utilización de tarjeta legítima, encontrada o sustraída a sus titulares*". No obstante, la Sentencia del Tribunal Supremo de 14 de julio de 1999, consideraba delito de estafa la utilización en un cajero de la tarjeta magnética sustraída a su titular.

B. Utilización de tarjeta de crédito sustraída o extraviada en establecimiento, sin cooperación por parte del empleado del establecimiento: Estafa y falsedad en documento mercantil. Ahora bien, la casuística jurisprudencial diferenciaba si el empleado del establecimiento, víctima del engaño, empleó o no la suficiente diligencia debida. Si la empleó no hay problema en afirmar la estafa. Si el empleado fue poco diligente en la labor de comprobar la identidad del sujeto que presenta la tarjeta y el cotejo de la firma, la jurisprudencia en

algunos casos consideraba que el engaño era tan burdo que no permitía la consideración de "bastante" para constituir el tipo de estafa, mientras que en otros casos a pesar de ello, calificó el hecho de estafa y falsedad en documento mercantil (como por ejemplo hacen las Sentencias de la Audiencia Provincial de Vizcaya -sección sexta- n. 65/2002, de 30 de enero, y n. 393/2001, de 7 de septiembre, o la Sentencia de la Audiencia Provincial de Cantabria -sección primera- n. 324/2013, de 29 de julio).

C. Utilización de tarjeta de crédito sustraída o extraviada en un establecimiento, con cooperación por parte del empleado del establecimiento. Calificar este caso como estafa era más complejo, pues no existía un sujeto pasivo al que el engaño provocase un error. Aquí el dependiente del establecimiento es un cooperador necesario del sujeto que usa ilegítimamente la tarjeta de crédito (o incluso un coautor). La solución debía estar más cercana a la de la utilización de la tarjeta de crédito en el cajero automático. En este caso "la máquina" a la que se accede no es el cajero, sino el terminal de la entidad bancaria en el establecimiento; de otro lado, el objeto material puede ser el bien adquirido fraudulentamente, o incluso dinero, si el empleado del establecimiento lo que hace es entregar dinero al portador de la tarjeta. Por lo demás la tarjeta lo que hace es facilitar el acceso al objeto material del delito de apoderamiento. No obstante, la Sentencia del Tribunal Supremo n. 2175/2001, de 20 de noviembre, también calificaba como falsedad y estafa la conducta de un empleado de una empresa encargada de hacer llegar a sus titulares tarjetas de crédito, que haciendo suya una se dirige al establecimiento mercantil, donde de acuerdo con trabajadores del mismo, utiliza la tarjeta para realizar compras, firmando el recibo de compra, que fue cargado en la cuenta del titular de la tarjeta. Consideró la sentencia que utilizar de forma ilegítima la tarjeta de crédito y en connivencia con terceros introducir datos en la máquina, para que por tal artificio engañoso obtener fondos de forma no consentida por el perjudicado, era constitutivo de la conducta de valerse de alguna manipulación informática para consentir la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero del artículo 248.2 CP. En el mimo sentido la Sentencia del Tribunal Supremo n. 692/2006, de 26 de junio, señalando que "*La conducta de quien aparenta ser titular de una tarjeta de crédito cuya posesión detenta de forma ilegítima y actúa en connivencia con quien introduce los datos en una máquina posibilitando que ésta actúe mecánicamente, está empleando un artificio para aparecer como su titular ante el terminal bancario a quien suministra los datos requeridos para la obtención de fondos de forma no consentida por el perjudicado. Y, en consecuencia, se encuentra incurso en la conducta definida en el art. 248.2 del Código Penal*".

D. Uso de tarjeta de crédito no devuelta a la empresa en la que ha rescindido el contrato. En este caso no hay falsedad, pues el acusado firmaba con su propio nombre. La Sentencia del Tribunal Supremo n. 1160/1999, de 14 de julio, consideró que se daban los requisitos del delito de estafa. Sin embargo, es discutible afirmar que aquí se dan los elementos de la estafa (relación de causalidad engaño-error-acto de disposición).

E. Uso fraudulento de la tarjeta de crédito por su propio titular. Sujeto que cambia de entidad bancaria y continúa usando la tarjeta de débito de la anterior entidad, sin saldo. La Sentencia de la Audiencia Provincial de Granada -sección primera-, n. 637/1998, de 1 de octubre, remitía la cuestión al ámbito del derecho civil o mercantil, señalando que la conducta del acusado no puede conducir al error, sino que esto sólo es posible por un error de la entidad, originado por su propia conducta y ajeno totalmente a la conducta del acusado.

Con la fórmula introducida por Ley Orgánica 5/2010, de 22 de junio en el nuevo artículo 248.2.c) CP en todas las situaciones descritas anteriormente se deberá calificar el hecho como estafa, incluso en la última señalada, en tanto que el tipo remite a "operaciones de cualquier clase", lo único determinante será que el hecho se realice utilizando tarjetas de crédito o débito o cheques de viaje o los datos en ellas incorporados. Así, por ejemplo, la Sentencia de la Audiencia Provincial de las Palmas (sección 6ª) de 28 de julio de 2015 (confirmada por Sentencia del Tribunal Supremo n. 749/2016, de 11 de octubre), dispone lo siguiente: "*En cuanto al delito de estafa, o alternativamente de robo con fuerza en las cosas, recordemos que el art. 248 fue redactado LO 5/2010, de 22 de junio y, por tanto, no estaba en vigor a la fecha de comisión de los hechos (durante la noche del 18 al 19 de mayo de 2010). En tal fecha, los hechos serían constitutivos, como ha calificado el Ministerio Fiscal de forma alternativa y la Acusación Particular de forma principal, de un delito de robo con fuerza en las cosas castigado en el artículo 238.4º en relación con el 239 y 240 del CP. Según la STS 427/99, de 16 de marzo y 666/99 de 29 de abril): <<es robo, y no estafa, el apoderamiento dinerario conseguido mediante la introducción en un cajero automático de una tarjeta de crédito, previamente sustraída, y cuyo número secreto se ha llegado a saber de alguna manera, porque se produce un apoderamiento de un bien ajeno sin la voluntad de su dueño y con uso de una llave falsa>>. Así las cosas, la actividad realizada por el acusado Lucas debe ser calificada como constitutiva de un delito continuado de robo con fuerza en las cosas del artículo 238.4º, por la utilización de llave falsa en su ejecución*".

De este modo, todas las operaciones fraudulentas realizadas con tarjetas o con los datos incorporados en ellas pasan a ser consideradas estafas del artículo 248.2.c) CP. Así, por ejemplo, las Sentencias de las Audiencias Provinciales de las Islas Baleares (sección primera) n. 28/2019, de 29 de marzo (utilizando una tarjeta en la que se habían incluido los datos de un tercero), de Navarra (sección primera) n. 301/2018, de 21 de diciembre y de Cantabria (sección primera) n. 347/2018, de 14 de septiem-

bre (utilizando en cajeros y comercios la tarjeta del denunciante), de Vizcaya (sección segunda) n. 5/2018, de 31 de enero, (en concurso de normas con el delito de falsedades del artículo 399 bis CP, al realizar compras con una tarjeta clonada), de Madrid (sección quinta) n. 64/2017, de 17 de julio, (por realizar trasferencias con cargo a la tarjeta de otro), de Madrid (sección cuarta) n. 222/2017, de 18 de mayo (por la empleada de hogar que, conociendo el número secreto de la empleadora, extraía dinero del cajero), o de Madrid (sección vigésimo novena), n. 193/2016, de 20 de abril (por realizar dos compras a través de internet mediante los datos de las tarjetas bancarias de la víctima), entre otras muchas.

4.2.4. Algunas actividades fraudulentas a través de Internet

Como en el resto de la vida social, Internet también en el ámbito delictivo, se ha convertido en una herramienta de información y comunicación de referencia a nivel mundial. La facilidad de información, comunicación y de intervención en relaciones comerciales y económicas, hace que también en el ámbito de la delincuencia patrimonial hayan aparecido nuevas formas comitivas, relacionadas con las transacciones comerciales fraudulentas, la banca electrónica, o el uso de los datos incorporados en tarjetas de crédito, debito u otras, por personas distintas a sus legítimos propietarios.

Son cientos, tal vez miles, las modalidades fraudulentas contra el patrimonio con las que se puede operar con Internet. No obstante, debe tenerse presente, que estas modalidades fácticas de desarrollar la conducta fraudulenta, en un lenguaje jurídico penal se van a reducir, en principio a dos: De un lado, formas de engaño bastante a través de Internet (por correo electrónico o a través de mensajes enviados por redes sociales u otras formas de comucación, por ejemplo), para hacer caer en el sujeto pasivo en el error que le hace hacer una disposición patrimonial en perjuicio suyo o de un tercero, en estos casos Internet servirá para facilitar la comisión del delito tradicional de estafa; de otro lado, otra modalidad fraudulenta, consistirá en obtener datos económicos del sujeto (por ejemplo claves de acceso a la banca electrónica) para que a través mecanismos informáticos u otro artificio semejante el sujeto activo realice la transacción patrimonial sin consentimiento de su titular.

La peligrosidad de estos fraudes tradicionales realizados con la asistencia de las tecnologías de la información y la comunicación, la aplicación de los algoritmos propios del big data y de la inteligencia artificial va a verse incrementada exponencialmente. Tanto en la propia materialización del engaño, como en el proceso de selección de las posibles víctimas del fraude.

En el ámbito del uso fraudulento patrimonial de Internet, el "Phishing" es la modalidad de estafa más común. Se trata de dirigirse al sujeto pasivo con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de

tarjeta de crédito, identidades, etc. para luego ser usados de forma fraudulenta. Son múltiples las formas de realización de este tipo de fraudes por Internet. El Phising, obviamente, no es exclusivo de Internet, en tanto que se trata de una conducta dirigida a obtener una información bancaria de un tercero, por lo que también suele considerarse tal el llamado Phising telefónico, mediante la solicitud de datos bancarios por teléfono con cualquier excusa. Idéntica conducta se realiza también en telefonía móvil, vía mensaje SMS o de Whatsapp, conocida como "Smishing".

Otros fraudes patrimoniales habituales a través de Internet, son el "Pharming" (gusanos o troyanos)[64], las "Cartas nigerianas"[65], el "Keylogger"[66] o las "Mulas"[67].

4.2.5. Características de estos fraudes

Son actividades fraudulentas tradicionales (ataques contra el patrimonio) que ven favorecida la ejecución con las tecnologías de la información y la comunicación y el big data. En general, presentan las siguientes características:.

- Normalmente implican una falsedad en la identificación o en la solvencia del sujeto (como en los fraudes tradicionales).
- El carácter transfronterizo que ofrecen las tecnologías de la información y la comunicación favorece la creación de organizaciones estratégicamente localizadas, que dificultan enormemente la investigación de estos delitos.
- La persecución de estos fraudes presenta graves dificultades, por que: a) No siempre existe una clara regulación legal, o la existente no siempre se interpreta correctamente; b) Se presentan dificultades técnicas para la investigación; c) Existen lagunas de formación en nuevas tecnologías en los departamentos de seguridad de las empresas, policía y jueces; d) El carácter transnacional de estos delitos dificulta enormemente su persecución; e) La mayor parte de estos delitos se basan sobre una identidad falsa o robada: Mediante identidades verdaderas suplantadas; Mediante identidades falsas creadas a partir de documentos auténticos; Mediante identidades totalmen-

[64] Consiste en la manipulación de las direcciones DNS para conseguir que las páginas que visiten los usuarios no sean las originales aunque su aspecto será idéntico. Al operar en esta Web los usuarios con sus nombres y contraseñas de acceso, entregan esta información al infractor.

[65] Se trata de una modalidad común de estafa por la que solicita a un sujeto que ingrese una cantidad de dinero en una cuenta para los trámites para cobrar un presunto premio de lotería que ha obtenido en otro país, o una herencia,…

[66] Se trata de la instalación tanto de programas como de dispositivos físicos que registran la actividad del teclado, con lo que el sujeto obtiene la información de modo ilícito.

[67] Una persona que transfiere dinero o mercancías que han sido obtenidas de forma ilegal en un país (generalmente a través de Internet), a otro país, donde suele residir el autor del fraude.

te inexistentes; Utilizando personas que permiten utilizar su propia identidad por un precio.

5. DELITOS RELACIONADOS CON EL CONTENIDO

El artículo 9 del Convenio sobre Ciberdelincuencia del Consejo de Europa establece que cada Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima una serie de conductas relativas a la pornografía infantil[68], sistematizadas del siguiente modo:

- **a.** Producción de pornografía infantil con vistas a su difusión por medio de un sistema informático.
- **b.** Oferta o puesta a disposición de pornografía infantil por medio de un sistema informático.
- **c.** Difusión o transmisión de pornografía infantil por medio de un sistema informático.
- **d.** Adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona.
- **e.** Posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

Ante la complejidad que supone la determinación terminológica del propio concepto de "pornografía infantil", el Convenio sobre Ciberdelincuencia del Consejo de Europa ofrece un concepto de pornografía infantil "flexible", que permitirá a los dis-

[68] En profundidad sobre el tema, vid. el excelente trabado de MORILLAS FERNÁNDEZ, D.L., Análisis Dogmático y Criminológico de los Delitos de Pornografía Infantil. Especial consideración de las modalidades comisivas relacionadas con Internet, Madrid 2005, y "Los delitos de pornografía infantil en el derecho comparado", Cuadernos de Política Criminal" 84, Madrid 2004, páginas 31 y siguientes,

También, MORALES PRATS, F.," Pornografía infantil e Internet: la respuesta en el Código Penal Español", Problemática jurídica en torno al fenómeno de Internet, Cuadernos de derecho Judicial 4, Madrid 2000, páginas 175 y siguientes, y "El derecho penal ante la pornografía infantil en Internet" Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet, Pamplona 2002, páginas 95 y siguientes; FERNÁNDEZ-PACHECO ESTRADA, C., "Pornografía infantil e Internet: ¿reto jurídico o problema social?", Revista general de legislación y jurisprudencia 2, Madrid 2006, páginas 245 y siguientes; FERNÁNDEZ TERUELO, D.G., "La sanción penal de la distribución de pornografía infantil a través de Internet", Boletín de la Facultad de Derecho de la UNED 2, Madrid 2000, páginas 259 y siguientes; REDONDO HERMIDA, A., "El delito de difusión de pornografía infantil por Internet", Diario La Ley, Nº 6591, Madrid 2006, pags. 1-5; ROJO GARCÍA, J.C., "La realidad de la pornografía infantil en Internet", Revista de Derecho Penal y Criminología" 9, Madrid 2002, páginas 211 y siguientes; MARTIN-CASALLO LÓPEZ, J., Actualidad informática Aranzadi: revista de informática para juristas,, Nº 40, 2001, pag. 3; ANARTE BORRALLO, E., "Incidencia de las nuevas tecnologías…, Ob. cit., páginas 221 y siguientes.

tintos Estados adaptar sus legislaciones al mismo. Así, se considera pornografía infantil: la representación visual de:

— Un menor comportándose de forma sexualmente explícita.

— Una persona que parezca un menor comportándose de forma sexualmente explícita.

— Imágenes realistas que representen a un menor comportándose de forma sexualmente explícita.

Considerando que por menor se entenderá persona menor de 18 años, si bien, se deja a la legislación nacional la posibilidad de establecer un límite inferior, estableciendo el mínimo -en todo caso- en *16 años*.

Al mismo tiempo, señala el Convenio sobre Ciberdelincuencia que cualquier Estado podrá reservarse el derecho a no aplicar en todo o en parte las conductas consistentes en la adquisición o posesión de este material para uso privado[69], así como la representación de una persona que parezca mayor o de imágenes realistas que representen a un menor.

Por su parte, en el ámbito de la Unión Europea, para permitir la aplicación de la Decisión de 29 de mayo de 2000, relativa a la lucha contra la pornografía infantil en Internet (2000/375/JAI), se elaboró de la Decisión Marco 2004/68/JAI del Consejo de 22 de diciembre de 2003 relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, que tenía por objeto aproximar las disposiciones legales y reglamentarias de los Estados miembros a la cooperación policial y judicial en materia penal, con el fin de luchar contra la trata de seres humanos, la explotación sexual de los niños y la pornografía infantil. En el marco de la Unión Europea esta decisión marco estableció un marco normativo común para abordar cuestiones tales como la tipificación penal, las sanciones, las circunstancias agravantes, la competencia y la extradición. En la línea del Convenio sobre Ciberdelincuencia del Consejo de Europa, se estableció la edad de 18 años para considerar "niño" a efectos de este tipo de delitos, y describiendo la pornografía infantil la representación visual de: un niño real practicando o participando en una conducta sexualmente explícita, incluida la exhibición lasciva de los genitales o de la zona púbica de un niño; una persona real que parezca un niño practicando o participando de la conducta anterior; o imágenes realistas de un niño inexistente practicando o participando de la conducta sexualmente explícita; Permitiendo que cada Estado pueda excluir de la responsabilidad penal cuando la persona real que parezca un niño tenga más de 18 años en el momento de la representación y cuando la posesión del material sea para uso privado y los niños hayan

[69] Al respecto, vid. ESQUINAS VALVERDE, P. "El tipo de mera posesión de pornografía infantil en el código penal español (Art. 189.2): razones para su destipificación", Revista de Derecho Penal y Criminología, 18, Madrid 2006, páginas 171 y siguientes.

alcanzado la mayoría de edad para consentir y hayan prestado su consentimiento y el caso de la producción de imágenes realistas de un niño inexistente, cuando sea para uso estrictamente privado.

La Decisión Marco 2004/68/JAI del Consejo de 22 de diciembre de 2003 relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, es sustituida por la Directiva 2011/92/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de menores y la pornografía infantil. Esta Directiva 2011/92/UE, en su artículo 2.c) define la pornografía infantil cómo: i)Todo material que represente de manera visual a un menor participando en una conducta sexualmente explícita, real o simulada; ii) toda representación de los órganos sexuales de un menor con fines principalmente sexuales; iii) 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; iv) 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.

Por su parte, el artículo 5 de la Directiva 2011/92/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de menores y la pornografía infantil, en sus apartados 2 a 6 recoge las infracciones relacionadas con la pornografía infantil, respecto de las que los Estados miembros se comprometen a adoptar las medidas necesarias para garantizar su punibilidad:

— La adquisición o posesión de pornografía infantil, con la previsión de una pena privativa de libertad de duración máxima de al menos un año.

— El acceso a sabiendas a pornografía infantil por medio de las tecnologías de la información u la comunicación, con la previsión de una pena privativa de libertad de duración máxima de al menos un año.

— La distribución, difusión o transmisión de pornografía infantil, con la previsión de una pena privativa de libertad de duración máxima de al menos dos años.

— El ofrecimiento, suministro o puesta a disposición de pornografía infantil, con la previsión de una pena privativa de libertad de duración máxima de al menos dos años.

— La producción de pornografía infantil, con la previsión de una pena privativa de libertad de duración máxima de al menos tres años.

La Directiva 2011/92/UE deja a discreción de los Estados miembros decidir si castigar las imágenes realistas de un menor participando en una conducta sexual-

mente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales, cuando la persona que parezca ser un menor resulte tener en realidad 18 años o más en el momento de obtenerse las imágenes; así como si en esos casos se castiga o no cuando dichas imágenes han sido producidas y están en manos de su productor para su uso privado, siempre que no se haya empleado material pornográfico de los apartados i) a iii) del artículo 2c), y que el acto no implique riesgo de difusión del material.

Como novedad, el artículo 6.1 de la Directiva 2011/92/UE, exige a los Estados miembros incorporar en su derecho interno el delito de "*embaucamiento de menores con fines sexuales por medios tecnológicos*", consistente en *¨la propuesta por parte de un adulto, por medio de las tecnologías de la información y la comunicación, de encontrarse con un menor que no ha alcanzado la edad de consentimiento sexual, con el fin de cometer una infracción contemplada en los artículos 3, apartado 4,*[70] *y en el artículo 5, apartado 6*[71]*, cuando tal propuesta haya sido acompañada de actos materiales encaminados al encuentro*", con la previsión de una pena privativa de libertad de duración máxima de al menos un año. En su apartado segundo el artículo 6 de la Directiva 2011/92/UE, exige incorporar como delito en su derecho interno "cualquier tentativa de un adulto, por medio de la tecnología de la información y la comunicación, de cometer las infracciones contempladas en el artículo 5, apartados 2[72] y 3[73], embaucando a un menor que no ha alcanzado la edad de consentimiento sexual para que le proporcione pornografía infantil en la que se represente a dicho menor", sin especificar una pena minima a imponer.

La Directiva 2011/92/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de menores y la pornografía infantil, se incorpora al Derecho interno en España a través de la Ley Orgánica 1/2015, de 30 de Marzo, especialmente, dando una nueva redacción al artículo 189 CP y con la introducción del nuevo artículo 183 ter. Si bien, no obstante, de forma específica respecto de la utilización de las tecnologías de la información y la comunicación se incluyen expresamente los artículos 183.3 CP (el embaucamiento de menores de 16 años con fines sexuales, a través de internet, teléfono o utilizando las tecnologías de la información y la comunicación) y 189.5 CP (acceso a pornografía infantil utilizando las tecnologías de la información y la comunicación).

---

[70] "Realizar actos de caracter sexual con un menor que no ha alcanzado la edad de consentimiento sexual".

[71] "La producción de pornografía infantil".

[72] "La adquisición o posesión de pornografía infantil".

[73] "El acceso a sabiendas a pornografía infantil por medio de las tecnologías de la información y la comunicación".

La producción, venta, distribución, exhibición, oferta o facilitación de la producción, venta, distribución o exhibición de pornografía infantil con vistas a su difusión por medio de un sistema informático, así como la posesión para estos fines, aparece tipificada en el apartado y b) del artículo 189.1 del Código Penal español, con la imposición de una pena privativa de libertad de uno a cinco años. En el artículo 189.1a) se castiga, entre otras conductas, la utilización de menores o personas con discapacidad necesitadas de especial protección para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte.

La adquisición de pornografía infantil por medio de un sistema informático para un tercero se encuentra también tipificada en el apartado b) del artículo 189.1 del Código Penal español, con la imposición de una pena privativa de libertad de uno a cinco años, en tanto que la misma la misma se realiza para la posterior distribución. La adquisición para su propio uso aparece tipificada en el artículo 189.5 CP, castigada con la pena prevista de tres meses a un año de prisión o multa de seis a dos años. En este caso se equipara la adquisición para uso propio con el acceso 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.

En los casos de los apartados a y b del artículo 189.1 CP en los que se den una serie de circunstancias (menor de 16 años, trato especialmente vejatorio, que represente menores o personas con discapacidad víctimas de violencia o intimidación…,) el Código penal prevé que la pena será de 5 a 9 años de prisión. (Artículo 189.2 CP).

En cuanto al concepto de pornografía infantil, en el artículo 189.1 segunda parte CP hace una transposición literal de la Directiva 2011/92/UE, estableciendo lo siguiente:

— 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.

— Toda representación de los órganos sexuales de un menor o una persona con discapacidad necesitada de especial protección con fines principalmente sexuales.

— Todo material que represente de forma visual a una persona que parezca ser un menor o una persona con discapacidad necesitada de especial protección 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 perezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.

— 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.

6. DELITOS RELACIONADOS CON INFRACCIONES DE LA PROPIEDAD INTELECTUAL Y DERECHOS AFINES

El artículo 10 del Convenio sobre Ciberdelincuencia del Consejo de Europa establece que cada Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones contra la propiedad intelectual, en la doble dirección asumida por los tratados internacionales en materia de protección de la propiedad intelectual, definiendo:

- De un lado, las infracciones contra la propiedad intelectual (derechos de autor) de obras literarias y artísticas a escala comercial y por medio de un sistema informático.
- Y, de otro lado, las infracciones contra la propiedad intelectual (derechos de autor) respecto de intérpretes, ejecutantes **y** fonogramas, a escala comercial y por medio de un sistema informático.

No obstante, el Convenio sobre Ciberdelincuencia permite que cada Estado utilice para la protección de los derechos derivados de la propiedad intelectual normas distintas al Derecho penal, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que le incumban.

En el Ordenamiento interno, 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 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 (reformada recientemente por las Leyes 21/2014, de 4 de noviembre, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil -BOE de 5 de noviem-

bre de 2014-, y 2/2019, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564, del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017).

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 CP, apartados a y b).

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.

En cualquier caso, para la consideración del hecho como delito se exige ánimo de lucro y perjuicio de tercero. Por "ánimo de lucro", como en el resto de los delitos de naturaleza patrimonial habrá de considerarse un "elemento subjetivo del injusto", equivalente "al propósito de obtener con la conducta una ventaja patrimonial ilícita", y por perjuicio de tercero que la conducta tenga "idoneidad suficiente para perjudicar a los titulares de los derechos de propiedad intelectual"[74].

[74] En este sentido, González Rus, J.J., "Protección penal de sistemas…, ob. cit., páginas 13-14.

Como novedad, respecto de la utilización de las tecnologías de la información y la comunicación, la Ley Orgánica 1/2015, de 30 de marzo, 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 lucro obtenido por los titulares de estas páginas web que hacían de intermediarios, normalmente no procedía directamente de la descarga o, incluso, de la visualización directa desde la página de contenidos (mediante el sistema de streaming) realizada por el usuario sin autorización del titular del derecho de propiedad intelectual o su cesionario, sino de la publicidad alojada en ellas. Ello, unido a que las modalidades de conducta típica cerrada recogidas en el anterior artículo 270 CP, se limitaban al plagio, distribución, reproducción, comunicación pública, exportación, importación o almacenamiento, hacía más difícil su persecución penal.

Sujeto activo del delito serán los proveedores de los servicios, siendo éstos cualquier persona física o jurídica que suministren alguno de dichos servicios y no sólo quienes lo hagan con carácter comercial, por lo que se trata de un delito común que puede realizar cualquier persona El resto de los elementos típicos (el "ánimo de obtener un beneficio económico directo o indirecto" y el actuar "en perjuicio de tercero") coinciden con el tipo básico del artículo 270.1 CP.

7. OTRAS ACTIVIDADES DELICTIVAS RELACIONADAS CON LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Al margen de los "ciberdelitos" relacionados en el Convenio sobre Ciberdelincuecia del Consejo de Europa, relativos a la intimidad, a la propiedad, al contenido -respecto de la pornografía infantil y de la actividad fraudulenta- y a la propiedad intelectual, otras muchas formas de delincuencia pueden verse facilitadas y realizadas a través de tecnologías de la información y la comunicación, especialmente la realizada a través de internet y la aplicación de procedimientos de inteligencia artificial, con las dificultades añadidas en la investigación y persecución de la actividad delictiva que implica el uso de la red y del "juego" de los algoritmos con dicha finalidad ilícita. Así, no es inusual la comisión de los delitos de amenazas y de coacciones[75] a través

[75] Al respecto, por ejemplo la Sentencia de la Audiencia Provincial de Sevilla núm. 138/2005 (Sección 4), de 15 marzo (Ponente: Dª. Margarita Barros Sansinforiano) señala lo siguiente: "*Los hechos son también constitutivos de la falta de amenazas del Art. 620.2º del Código Penal que solicita la acusación particular, pues de las declaraciones de la denunciante resulta que el inculpado la amenazó con poner en Internet un vídeo que al parecer tenía grabado, en el que se veía a la denunciante manteniendo relaciones sexuales con el acusado, lo que produjo en la víctima, el natural desasosiego e intranquilidad, y que merece asimismo el reproche penal previsto en el referido precepto*"; en sentido similar califica como delito de delito de coacciones del artículo 172 CP la Sentencia de la Audiencia Provincial de Zaragoza núm. 374/2003 (Sección 1), de 20 noviembre (Ponente: D. Rubén Blasco Obedé), ante los siguientes hechos probados: "*Probado y así se declara que, el acusado José Miguel, mayor de edad, y sin antecedentes penales, que había mantenido una relación sentimental durante varios años con Amanda, que cesó en el mes de febrero de 2000, trabajando ambos en las oficinas de Comisiones Obreras de Aragón, sitas en Paseo de Constitución n° 12 de esta ciudad, molesto con esta ultima, y con sus amigas Cristina, Rebeca y Lidia, y con la intención de causarles el natural malestar, e intranquilidad, provocando una ruptura entre el grupo de amigos que estaba constituido, desde el día 1/12/2000, comenzó a,enviarles, a través de Internet,*

de mensajes de correo electrónico, o con publicidad a través de las redes sociales o en una página Web, o la comisión de conductas por estos medios constitutivas de los delitos contra el honor[76]. En este sentido, aun siguiendo la clasificación del Convenio del Consejo de Europa sobre Ciberdelincuencia de 2003, el Estudio sobre la cibercriminalidad en España de 2019, añade expresamente otras categorías dentro de la "ciberdelincuencia", tales como los delitos contra el honor y las amenazas y coacciones[77].

De otro lado, el uso de las tecnologías de la información y la comunicación pone en manos de la criminalidad organizada un instrumento que facilita su finalidad delictiva. En este sentido las nuevas tecnologías vienen a facilitar los canales de información y organización de la llamada criminalidad organizada, incluyendo el narcotráfico, el terrorismo, el blanqueo de capitales, el tráfico de armas, el tráfico de personas, entre otras actividades propias de la delincuencia transfronteriza.

En esta línea, en el ámbito de las actividades terroristas, especialmente tras el atentado contra las Torres Gemelas del 11 de septiembre de 2001, se viene acuñando el término de "ciberterrorismo", para referirse a la utilización de Internet y las tecnologías de la información y la comunicación por grupos y organizaciones terroristas. En esta línea, se podría definir el Ciberterrorismo, como la forma de terrorismo que utiliza las tecnologías de información y la comunicación para intimidar, coaccionar o para causar daños a grupos sociales con fines políticos o religiosos[78]. En particular, al margen de la actividad que pudiera catalogarse propiamente como ciberdelincuencia, estas organizaciones criminales en el ámbito de su función organizativa y de información, pueden utilizar las tecnologías de la información y la comunicación y sobre todo las posibilidades que ofrecen las herramientas de Internet y el big data, entre otras actuaciones, para lo siguiente:

- Para reclutar adeptos, recaudar fondos y lanzar una campaña de intimidación a escala mundial.

---

mensajes a los teléfonos móviles de dichas personas, con frases de contenido sexual, perturbando su vida diaria".

[76] En este sentido, por ejemplo, la Sentencia de la Audiencia Provincial de Asturias núm. 174/2004 (Sección 2), de 20 mayo (Ponente: Dª. Covadonga Vázquez Llorens), calificaba como delito de calumnias con publicidad del artículo 212 CP la publicación en foro de página Web de Internet de una información en la que se imputaba a la querellante la apropiación de fondos pertenecientes a una sociedad, que pudiera ser constitutiva de un delito de malversación de caudales o fraude de subvenciones.

Al respecto, vid. Ort. Berenguer, E./ Roig Torres, M., Delitos informáticos y delitos comunes cometidos a través de la informática, Valencia 2001, página 146.

[77] Estudio sobre la cibercriminalidad..,., ob. cit., página 17.

[78] En otro contexto, también se ha denominado "Ciberterrorismo" "a la introducción de virus en la red capaces de infectar a miles de ordenadores en todo el mundo". Al respecto, Quintero Olivares, G., "Internet y propiedad intelectual", Internet y Derecho penal, Cuadernos de Derecho Judicial, 10, Madrid 2001, página 371.

- Recopilar información de los objetivos de las organizaciones terroristas. Por medio de Internet pueden averiguar los horarios y la localización de objetivos, en tiempo real desde cualquier lugar del mundo, tales como servicios de transporte, centrales nucleares, edificios públicos, aeropuertos y puertos, así como las medidas antiterroristas.
- Internet se convierte en una herramienta de comunicación y formación en la actividad terrorista, permitiendo contacto inmediato entre los distintos estamentos de la organización (distribución de instrucciones y manuales para elaborar explosivos…).
- Favoreciendo el adiestramiento en el fanatismo del terrorismo integrista.
- La utilización de algoritmos facilita la realización de las conductas de reclutamiento, de recaudación de fondos, de selección de objetivos, ...a las organizaciones terroristas.

CONCLUSION

La imposibilidad de limitar el uso ilícito y fraudulento de las tecnologías de la información y la comunicación es la razón por la que el Código penal español no incluye específicamente un Título o un Capítulo rubricado específico sobre la materia, que podría tener alguna de las rubricas siguientes: "de los delitos informáticos", "de los delitos relativos a la informática", "de los delitos relativos a la sociedad de la información y la comunicación", o "de los ciberdelitos". Tratar de incluir todas las posibilidades delictivas imaginables a través de las tecnologías de la sociedad de la información y la comunicación en una única parte del Código penal, en aras a una mayor organización y sistematización de los tipos penales conduciría sencillamente al fracaso legislativo.

No obstante, a lo largo del articulado del Código Penal se encuentran diseminados multitud de tipos penales cuya comisión puede ser incluida dentro del término coloquial de "delincuencia informática", "criminalidad informática", "ciberdelincuencia" o "cibercriminalidad", por lo cual, en la descripción de la conducta típica se hace expresa referencia a esta modalidad delictiva, cuando con la redacción tradicional no se incluía (como ocurre, por ejemplo, con los delitos contra la intimidad, en los llamados daños informáticos o en determinados delitos contra la indemnidad sexual de los menores).

Así, puede afirmarse, sin riesgo de caer en error, que -en la mayoría de los casos- se considera que la sociedad tecnológica permite modalidades de conducta novedosas que afectan a bienes jurídicos tradicionales (intimidad y privacidad, propiedad, indemnidad sexual…), por lo que lo que se hace es modificar los tipos

penales existentes describiendo conductas que incluyan las nuevas formas comisivas.

BIBLIOGRAFIA

AA.VV. Morillas Cueva (dir.), Sistema de Derecho Penal. Parte Especial, Madrid 2020

AA.VV., *Delincuencia informática: tiempos de cautela y amparo*, Madrid 2012

ÁLVAREZ VIZCAYA, M., "Consideraciones político criminales sobre la delincuencia informática: El Papel del Derecho penal en la red", Internet y Derecho penal, Cuadernos de Derecho Judicial, 10, Madrid 2001

BENITEZ ORTUZAR IF. "Informática y delito". Aspectos penales relacionados con las nuevas tecnologías, en Benitez Ortúzar (dir.) *Reforma del Código penal. Respuestas para una sociedad del siglo XXI*

BENÍTEZ ORTUZAR, I.F. en "De los daños", en Morillas Cueva (Dir.) *Estudios sobre el Código penal reformado (leyes orgánicas 1/2015 y 2/2015*), Madrid 2015

CASTELLÓ NICÁS, N., en "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio y delitos contra el honor", en Morillas Cueva (Dir.) *Estudios sobre el Código penal reformado (leyes orgánicas 1/2015 y 2/2015*), Madrid 2015

CASTILLO JIMÉNEZ, C., "Protección del Derecho a la Intimidad y uso de las nuevas tecnologías de la información"; Derecho y Conocimiento, n. 1

DE LA CUESTA ARZAMENDI, J,L./DE LA MATA BARRANCO N.J. (Coords.) *Derecho penal informático,* Madrid 2010

DE LA MATA MARTÍN, R., *Delincuencia informática y Derecho penal*, Madrid 2012.

FERNÁNDEZ-PACHECO ESTRADA, C., "Pornografía infantil e Internet: ¿reto jurídico o problema social?", Revista general de legislación y jurisprudencia 2, Madrid 2006

FERNÁNDEZ TERUELO, D.G., "La sanción penal de la distribución de pornografía infantil a través de Internet", Boletín de la Facultad de Derecho de la UNED 2, Madrid 2000

GALÁN MUÑOZ, A., El fraude y la estafa mediante sistemas informáticos, Valencia 2004

MARTIN-CASALLO LÓPEZ, J., Actualidad informática Aranzadi: revista de informática para juristas,, Nº 40, 2001

MORALES PRATS, F.," Pornografía infantil e Internet: la respuesta en el Código Penal Español", Problemática jurídica en torno al fenómeno de Internet, Cuadernos de derecho Judicial 4, Madrid 2000

MORALES PRATS, F., "El derecho penal ante la pornografía infantil en Internet" Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet, Pamplona 2002.

MORILLAS FERNÁNDEZ, D.L., Análisis Dogmático y Criminológico de los Delitos de Pornografía Infantil. Especial consideración de las modalidades comisivas relacionadas con Internet, Madrid 2005

MORILLAS FERNÁNDEZ, D.L., "Los delitos de pornografía infantil en el derecho comparado", Cuadernos de Política Criminal" 84, Madrid 2004

PAVÓN PÉREZ, J.A., "La labor del Consejo de Europa en la lucha contra la cibercriminalidad: El protocolo adicional al Convenio sobre Cibercriminalidad relativo a la incrimi-

nación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos", Universidad de Extremadura. Anuario de la Facultad de Derecho, vol. XXI, 2003

REDONDO HERMIDA, A., "El delito de difusión de pornografía infantil por Internet", Diario La Ley, Nº 6591, Madrid 2006

ROJO GARCÍA, J.C., "La realidad de la pornografía infantil en Internet", Revista de Derecho Penal y Criminología" 9, Madrid 2002

SOLARI MERLO, M.N., "Análisis de los delitos informáticos. una propuesta de clasificación", en *Revista de Derecho y Proceso penal*, n. 60, 2020

VELASCO NUÑEZ, E./SANCHÍS CRESPO, C., *Delincuencia informática. Tipos delictivos e investigación criminal*, Valencia 2019