Universidad Zaragoza
1542

Trabajo Fin de Grado

Daños informáticos: análisis de los artículos 264 y 264 bis del Código Penal

Computer damage: analysis of articles 264 and 264 bis of the Criminal Code

Autora

María Iturbide Gil

Directora

Estrella Escuchuri Aisa

Facultad de Derecho

Junio 2022

ÍNDICE

ABREVIATURAS

Adpo.	Apartado
Art.	Artículo
Arts.	Artículos
CE	Constitución Española
Coord	Coordinador
Coords	Coordinadores
ENISA	European Union Agency for Network and Information Security
INTERPOL	Organización Internacional de Policía Criminal
LCEur	Legislación de las Comunidades Europeas
núm.	Número
p.	Página
pp.	Páginas
ss.	Siguientes
TIC	Tecnologías de la Información y Comunicación
UE	Unión Europea
OCDE	Organización para la Cooperación y el Desarrollo Económico
UIT	Unión Internación de Telecomunicaciones

I. INTRODUCCIÓN

El presente trabajo de fin de grado, bajo el título «Daños informáticos: análisis de los artículos 264 y 264 bis del Código Penal», pretende aproximarse al fenómeno de la denominada ciberdelincuencia y, en particular, analizar el marco jurídico-penal de los daños a datos o programas informáticos y los daños a los propios sistemas informáticos (también se alude a los daños informáticos con la expresión sabotaje informático). Antes del estudio de los preceptos citados, trataremos de entender el presente debate sobre el concepto de «delito informático» o «ciberdelito» e incluso conocer cuál es la situación actual en nuestro país con respecto a las actuaciones ilícitas vinculadas al uso de las tecnologías de la información y la comunicación.

Sin duda, el nacimiento de Internet constituye uno de los hitos más importantes del siglo XX. Es a finales de los años 60 cuando se establece la primera red de comunicación segura para transferir documentos y datos entre los diferentes sistemas del Departamento de Defensa de Norteamérica. A lo largo de los siguientes años, se desarrollaron diferentes protocolos de comunicación dando como resultado, en el año 1991, la creación del World Wide Web (comúnmente conocido como www), una herramienta de comunicación que culminaría en el surgimiento de la denominada «sociedad de la información». En este contexto, se impuso la idea de que, a través de las nuevas tecnologías, podría desempeñarse un trabajo más efectivo, eficaz y democrático.

De lo dicho, se deduce que las nuevas tecnologías supusieron una revolución en la relación entre la Administración y la ciudadanía en tanto en cuanto gran parte del proceso administrativo se desarrolla, a día de hoy, a través de Internet. De acuerdo con lo señalado en el Considerando 1 de la Directiva (UE) 2016/1148 (LCEur 2016, 1042) del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión: «Las redes y sistemas de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para las actividades económicas y sociales, y en particular para el funcionamiento del mercado interior».

Ahora bien, esta transición de lo analógico a lo digital no está exenta de problemas puesto que ha dado lugar a la proliferación de nuevos riesgos. Atendiendo al informe realizado por INTERPOL en el año 2020 en cuanto a los efectos de la COVID-19 en la ciberdelincuencia[1], esta ha evolucionado de tal manera que se han creado «nuevos ataques e intensificado su ejecución» debido a la dependencia de la conectividad en los momentos de confinamiento de la población.

Es por ello de especial relevancia conocer cómo se articula la respuesta a estas nuevas formas de delincuencia en nuestro ordenamiento jurídico. Así, en un primer momento realizaremos un análisis sobre el concepto de ciberdelito, pues existe actualmente un fuerte debate sobre su definición y alcance. En un segundo punto, veremos cuál es la situación en España respecto a las conductas ilícitas realizadas a través de Internet de la mano del Informe sobre Cibercriminalidad realizado por el Ministerio de Internet. Posteriormente, nos centraremos en el marco jurídico de estas figuras a nivel internacional, europeo y nacional para, en cuarto lugar, analizar específicamente los artículos 264 CP y 264 bis CP junto a varias sentencias de especial relevancia.

II. CONCEPTO DE CIBERDELITO

Como ya hemos mencionado, el nacimiento de Internet y, el consecuente tratamiento automatizado de los datos, generó múltiples beneficios, así como riesgos. Tal como expone MATA Y MARTÍN[2], esta situación generó un riesgo especial en torno a la protección de los intereses fundamentales de los individuos. Es por ello que la doctrina plantea la necesidad de que el Derecho en general, y también el Derecho penal, no permanezcan ajenos a esta realidad. En este sentido, FLORES PRADA considera fundamental regular su uso con

[1] INTERPOL, *Ciberdelincuencia, efectos de la COVID-19,* 2020 accesible en https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

[2] MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, p. 17.

«normas jurídicas eficaces y vinculantes que garanticen los principios y valores de los modernos ordenamientos jurídicos»[3].

Precisamente por esta cuestión resulta esencial delimitar el objeto de análisis, conociendo qué se entiende por delitos informáticos y qué características poseen. Antes que nada, hay que hacer una precisión respecto a la terminología. Inicialmente se utilizó la expresión delito informático, pero desde los años 90, se recurre con más frecuencia al término ciberdelito o cibercrimen[4]. Como todavía se siguen utilizando ambos, en este trabajo los utilizaremos de forma indistinta. Así, en primer lugar, debemos poner de relieve el debate existente en la actualidad acerca de definición de ciberdelito. Aunque no existen disposiciones legales que determinen las características o elementos de un delito informático, son múltiples las referencias que, en la doctrina, jurisprudencia e incluso en la literatura se hacen al delito informático[5].

Un importante sector entiende que no resulta adecuado hablar de «delito informático» como concepto autónomo[6] ya que en nuestro Código Penal no existe ningún título específico que regule dichos delitos. Indica HERNÁNDEZ DÍAZ[7] que el legislador ha optado por diferenciar la comisión de ciertas conductas a través de la vía informática dentro del articulado de castigo de dichas conductas, en lugar de tipificar una acción u omisión cometida a través de medios informáticos como un delito individual. Así, el denominado delito informático –aquella infracción, penada por ley, que tiene relación con un bien o servicio informático[8]– no se recoge como categoría autónoma en el Código Penal ni en

[3] FLORES PRADA, I., *Criminalidad informática*, Tirant lo Blanch, Valencia, 2012, p. 25. También en el mismo sentido, entre otros, PICOTTI, L., «Ciberespacio y Derecho penal», en CANCIÓ MELIÁ y otros, *Libro Homenaje al Prof. Dr. Agustín Jorge Barreiro*, UAM, 2019, pp. 1195-1196.

[4] MIRÓ LLINARES, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, Madrid, 2012, pp. 37 y 38, propuso sustituir la referencia a «delitos informáticos» por los de cibercrimen y cibercriminalidad pues el riesgo no se sitúa en la utilización de tecnologías informáticas o en la información del sistema informático, sino en el sistema de redes telemáticas intercomunicadas y en las interrelaciones que allí se configuran. Véase sobre esto GIL GIL, A./HERNÁNDEZ BERLINCHES, R., *Cibercriminalidad*, Dykinson, Madrid, 2019, pp. 154-155.

[5] DAVARA RODRÍGUEZ, M. A., *Manual de Derecho Informático*, Aranzadi, Pamplona, 2015, p. 411.

[6] En este sentido, HERNÁNDEZ DÍAZ, L., «Aproximación a un concepto de derecho penal informático», en DE LA CUESTA ARZAMENDI y DE LA MATA BARRANCO, N., *Derecho penal informático,* Civitas, Madrid, 2010, p. 42.

[7] *Ibid.*, p. 43.

[8] Apartados 2 y 3 del artículo 197, artículos 197 bis, 197 ter, 197 quater, 197 quinquies, 264, 264 bis, 264 ter, entre otros del Código Penal vigente.

ninguna otra norma que se pudiera encuadrar en la legislación penal; por lo que no se podría hablar de «delito informático».

No obstante, otro sector de la doctrina –como por ejemplo DAVARA RODRÍGUEZ[9]–, estima necesario acudir a la nomenclatura de «delito informático» para poder realizar su estudio definiéndolo como «la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software». DE URBANO CASTRILLO[10], por su parte, entiende que de denominarlo como «delito informático», este debería tratarse como «el [acto] cometido a través de las TICs cuyos soportes evolucionan sin cesar: teléfono, televisión, móvil, ordenador, internet, y toda clase de dispositivos móviles conectados a la www, que posibilitan generar texto, sonido e imagen».

Lo cierto es que en la doctrina jurídica se sugieren definiciones más amplias que permiten explicar comportamientos diversos. Así, GALÁN MUÑOZ[11] entiende que debemos elaborar un concepto de delito informático que abarque tanto las figuras que incorporan el atentado contra sistemas informáticos, las que exigen su comisión por medio de dichos sistemas como también las que, aun no aludiendo a la comisión por medios informáticos, se cometen frecuentemente por las mencionadas vías. Así pues, se presentaría una «categoría criminológica»[12] que sería el reflejo del aumento del uso de las nuevas tecnologías y su consecuente empleo como medio para la comisión de distintos delitos. Un concepto así permite dar cabida tanto a los ciberdelitos propios (aquellos en los que por medio de las TIC se atenta contra los sistemas informáticos y las redes) y los ciberdelitos impropios (aquellos

[9] DAVARA RODRÍGUEZ, M. A., *Manual de Derecho Informático*, *cit.*, pp. 414-415.

[10] DE URBANO CASTRILLO, E., «El acoso y la delincuencia informática», *Revista Aranzadi Doctrinal* núm. 3, 2018, p. 42.

[11] GALÁN MUÑOZ, A., «*Compliance* frente a delitos informáticos», en *Estudios penales en homenaje al Prof. José Manuel Lorenzo Salgado*, ABEL SOUTO/BRAGE CENDÁN/GUINARTE CABADA/MARTÍNEZ-BUJÁN PÉREZ/VÁZQUEZ-PORTOMEÑE SEIJAS, Tirant lo Blanch, Valencia, 2021, p. 562.

[12] Nomenclatura expresada por MATA Y MARTÍN, R. M., «Avances tecnológicos y evaluación de nuevas necesidades iniciales de tutela penal», en ABEL SOUTO/BRAGE CENDÁN/GUINARTE CABADA/MARTÍNEZ-BUJÁN PÉREZ/VÁZQUEZ-PORTOMEÑE SEIJAS *Estudios penales en homenaje al Prof. José Manuel Lorenzo Salgado*, Tirant lo Blanch, Valencia, 2021, p. 908.

en los que el uso de las TIC es el medio comisivo para atentar contra bienes jurídicos, individuales o colectivos, cuando además este medio constituya un elemento esencial).

Respecto a la clasificación de los delitos pueden seguirse distintos criterios. Aquí vamos a exponer la propuesta por MIRÓ LLINARES. Este autor ha definido la ciberdelincuencia como «cualquier delito en el que las TIC juegan un papel determinante en su concreta comisión, que es lo mismo que afirmar que lo será cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan», y a partir de esta idea ha propuesto una clasificación en torno a dos variables: incidencia de las TIC en el comportamiento criminal y el móvil y contexto criminológico[13]. Así, encontramos las siguientes modalidades de cibercrimen.

[13] MIRÓ LLINARES, F., *El cibercrimen, cit.*, pp. 44 y 51 y ss.

Tabla 1.1.: Ejemplos ciberataques conforme a la clasificación en dos variables.

		CIBERATAQUES PUROS	**CIBERATAQUES RÉPLICA**	**CIBERATAQUES DE CONTENIDO**
		Conductas ilícitas cuyo único medio de comisión son las TIC	Conductas que ya se realizaban de otro modo en el espacio físico.	La infracción la constituye la información que se comparte.
CIBERATAQUES ECONÓMICOS	Comportamientos criminales llevados a cabo con la finalidad de obtener un beneficio patrimonial.	• Hacking • Malware • Ataques de insiders • Spam	• Ciberfraudes • Ciberblanqueo de capitales • Ciberocupación	• Distribución de pornografía infantil • Ciberpiratería intelectual
CIBERATAQUES SOCIALES	Delitos relacionados con actos de vida social que los individuos desarrollan en Internet.		• Ciberbulling • Ciberamenazas • Sexting	
CIBERATAQUES POLÍTICOS	Ataques con fines políticos contra los sistemas de información	• Ataques DoS • Malware intrusivo	• Ciberespionaje • Ciberguerra	• Discurso de odio • Ciberterrorismo

Fuente: Elaboración propia a partir de MIRÓ LLINARES, F., *El cibercrimen*, *cit.*, pp. 51 y ss.

Dentro de la variable de la incidencia de las TIC en el comportamiento criminal, encontramos tres premisas de clasificación:

1. El ciberataque puro, integrador de todas las conductas ilícitas que solo pueden ser cometidas a través de las nuevas tecnologías; serían figuras que nacen de la existencia de los propios sistemas informáticos. Dentro de esta subcategoría encontraríamos por ejemplo el *hacking*, entendido este como la violación de datos empresariales o particulares que se encuentran en la nube.

2. Una segunda premisa serían los ciberataques réplica, conductas que ya se daban en la realidad física antes de la introducción de las nuevas tecnologías y que, actualmente, se han adaptado a dichos novedosos medios. Los ciberfraudes o el phishing entrarían dentro de esta categoría, pues, como comentábamos, ya se daban en la realidad física.

3. Por último, los ciberataques de contenido constituirían un apartado de los ciberataques réplica, pero, debido a su importancia componen una subcategoría independiente. Estos comprenden aquellas infracciones cuyo contenido genera el acto ilícito, entre los que encontraríamos la incitación al odio en el ciberespacio, el ciberterrorismo o la piratería intelectual a través de Internet.

Esta subclasificación se relaciona con la variable del móvil y contexto criminológico a través del concepto de cibercrimen económico, cibercrimen social y cibercrimen político; entendidos estos como comportamientos criminales llevados a cabo con la finalidad de obtener un beneficio patrimonial, delitos relacionados con actos de vida social que los individuos desarrollan en Internet y ataques con fines políticos contra los sistemas de información, respectivamente.

LLORIA GARCÍA estima adecuada la clasificación realizada por MIRÓ LLINARES. Asimismo, destaca que no existe ningún punto en común (ni el bien jurídico ni el objeto material) entre los distintos delitos susceptibles de ser denominados como tecnológicos, excepto el de ser realizados a través de medios tecnológicos (ya sea el medio comisivo o el lugar donde se produce el ataque). Sin embargo, para acotar más el concepto –de modo que el hecho de que aparezca un elemento tecnológico no determine ya que se trate de un delito informático–, considera necesario analizar qué rasgos característicos cumplen las distintas actuaciones y qué consecuencias se derivan de las mismas. Así, serían delitos informáticos aquellos que «bien por el objeto material (sistema informático) o bien por el bien jurídico (seguridad de los sistemas informáticos) o bien por el medio comisivo (el tecnológico) o bien por el lugar en el que se producen (el ciberespacio) van acompañados de una especial

dificultad en su persecución y castigo y de un especial peligro de incremento de lesión del bien jurídico»[14].

Como vemos, se proponen dos elementos como determinantes de la inclusión en delitos informáticos de las distintas conductas. Por un lado, la dificultad en la persecución y por otro, el incremento de lesión. Con respecto a la dificultad de la persecución, esta viene determinada por la descentralización de los sujetos que ejecutan los ataques, ya que en múltiples ocasiones los delitos son realizados por numerosos sujetos situados en distintos países. A ello se le suma la dificultad existente para determinar la competencia debido a dicha transnacionalidad. Por otro lado, encontramos que estas conductas se realizan bajo un anonimato que entorpece la determinación de los sujetos y, por último, los autores suelen emplear técnicas que no dejan rastro de sus actuaciones y por tanto nos enfrentamos ante una cierta volatilidad de la prueba. Además, ciertas características de los delitos informáticos harían que se produjese un incremento de lesión del bien jurídico. En este sentido, el anonimato y la rápida reproducción de los daños podría generar una importante indefensión por parte de la víctima y, sobre todo, un incremento de los sujetos pasivos afectados o incluso de las consecuencias cuantitativas del delito. Por otro lado, también aumenta la lesión del bien jurídico el hecho de que, en ocasiones, los actos realizados en internet son permanentes[15,16].

Una vez efectuado el análisis de varios puntos de vista, en este trabajo de fin de grado entenderemos como «delito informático» lo expuesto por la Estrategia Nacional de Ciberseguridad de 2019[17] que, si bien no habla de delito informático, define el término de cibercriminalidad como el «conjunto de actividad 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».

---

[14] LLORIA GARCÍA, P., «Algunas reflexiones sobre el concepto de delito tecnológico y sus características», en GONZÁLEZ CUSSAC, J. L. (Dir.)/LEÓN ALAPONT J. L. (coord.), *Estudios jurídicos en memoria de la profesora doctora Elena Górriz Royo*, Tirant lo Blanch, Valencia, 2020, p. 507.

[15] Ibid., pp. 507-508.

[16] Hecho patente sobre todo en aquellos delitos relacionados con el honor, la intimidad o la integridad moral.

[17] Estrategia Nacional de Ciberseguridad 2019. Consultar en https://www.ccn-cert.cni.es/pdf/documentos-publicos/3809-estrategia-nacional-de-ciberseguridad-2019/file.html

Ahora bien, hablemos de delito informático, cibercriminalidad o de delitos cometidos a través de medios informáticos, es evidente que es necesaria una respuesta penal para hacer frente a los, cada día más comunes, ataques informáticos, tanto a pequeñas empresas o individuos, como a grandes corporaciones o administraciones. Con todo, como señala ROMEO CASABONA, «la adopción de reacciones penales ha de basarse escrupulosamente en el principio de proporcionalidad, teniendo en este caso como referente la mínima interferencia en la libertad de expresión, el respeto de la intimidad y de los datos personales, y el libre flujo de las comunicaciones telemáticas»[18].

Es por ello que en el siguiente epígrafe veremos cual es la incidencia actual de los delitos informáticos en España para posteriormente pasar a analizar las figuras delictivas relacionadas con los daños informáticos.

III. EVOLUCIÓN DE LA CIBERCRIMINALIDAD EN ESPAÑA

Antes de entrar a estudiar el análisis jurídico de los delitos informáticos es necesario conocer cuál es la realidad social referida a los mismos. Gracias a la publicación periódica del Informe sobre Criminalidad realizado por el Ministerio de Interior, somos capaces de entender la importancia que tienen en la actualidad. Así, el VIII Informe sobre Cibercriminalidad recoge los datos del año 2020 sobre los delitos informáticos recogidos por el Sistema Estadístico de Criminalidad (SEC) y por la Oficina de Coordinación de Ciberseguridad, ambas oficinas pertenecientes al Ministerio de Interior[19].

[18] ROMEO CASABONA, C. M.ª, «De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal», en ROMEO CASABONA (Coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Comares, 2006, p. 37. También para MATA Y MARTÍN, R. M., «Avances tecnológicos y …, *cit*., p. 908, no toda acción de ataque a la Red o mediante la Red tendrá que considerarse constitutiva de delito, sino que deberá respetar los principios de lesividad, subsidiariedad, fragmentariedad y proporcionalidad.

[19] Un estudio de los datos relativos a ciberdelincuencia desde el año 2011 al 2018 puede verse en CEREZO DOMÍNGUEZ, A. I./GARCÍA CORNEJO, R., «La ciberdelincuencia en España: un estudio basado en las estadísticas policiales», *Revista Electrónica de Estudios Penales y de la Seguridad*, 6, 2020. Disponible en https://www.ejc-reeps.com

La clasificación de las diferentes conductas se realiza conforme a las categorías establecidas por el Convenio de Budapest[20], que posteriormente abordaremos, añadiendo los delitos contra el honor y las amenazas y coacciones. De esta forma, en el año 2020 los delitos para cuya comisión se emplearon tecnologías de la información y comunicación aumentaron un 31,9% frente a los cometidos en el año 2019. Este aumento también se refleja en la tasa de delitos informáticos sobre el conjunto de la criminalidad, en el año 2016 representaba un 4,6% frente al 16,3% en el año 2020.

Entrando en detalle sobre cada categoría delictiva, encontramos que el 89,6% de las infracciones están relacionadas con el fraude informático. Si bien desde el año 2016 este había sido la infracción más cometida, vemos un aumento en el año 2020 con respecto al 2016 del 267,50%.

Tabla 3.1 Evolución de hechos conocidos por categorías delictivas

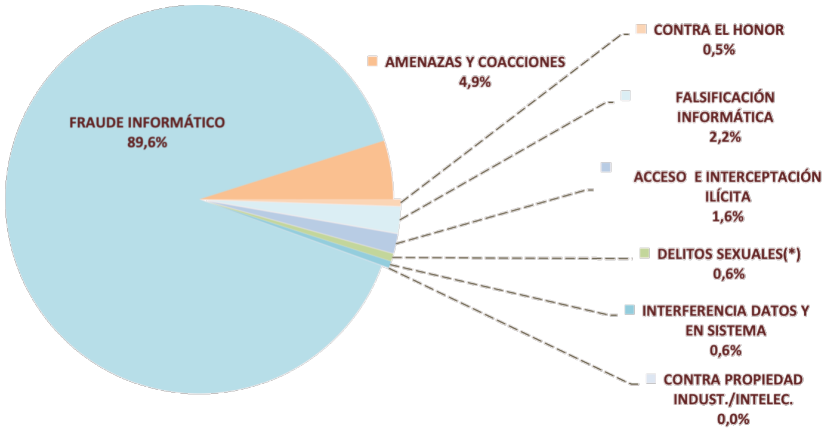
HECHOS CONOCIDOS	2016	2017	2018	2019	2020
ACCESO E INTERCEPTACIÓN ILÍCITA	3.243	3.150	3.384	4.004	4.653
AMENAZAS Y COACCIONES	12.036	11.812	12.800	12.782	14.066
CONTRA EL HONOR	1.546	1.561	1.448	1.422	1.550
CONTRA PROPIEDAD INDUST./INTELEC.	129	121	232	197	125
DELITOS SEXUALES(*)	1.231	1.392	1.581	1.774	1.783
FALSIFICACIÓN INFORMÁTICA	3.017	3.280	3.436	4.275	6.289
FRAUDE INFORMÁTICO	70.178	94.792	136.656	192.375	257.907
INTERFERENCIA DATOS Y EN SISTEMA	1.336	1.291	1.192	1.473	1.590
Total HECHOS CONOCIDOS	**92.716**	**117.399**	**160.729**	**218.302**	**287.963**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

Fuente: Estudio sobre la Cibercriminalidad en España 2020 – Ministerio de Interior.

[20] Véase el Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, en Budapest el 23 de noviembre de 2001 («BOE» núm. 226, de 17 de septiembre de 2010).

Gráfico 3.1 Evolución de hechos conocidos por categorías delictivas



Fuente: Estudio sobre la Cibercriminalidad en España 2020 – Ministerio de Interior.

Ahora bien, en la actualidad no solo nos encontramos con conductas delictivas relacionadas con los medios informáticos que afectan los individuos, sino que en múltiples ocasiones son las empresas e infraestructuras críticas las perjudicadas. Muestra de ello es el aumento de los ataques tipo malware y DDos en el año 2020 con respecto al año 2019 (40,42% frente a 20,29%). Así, los sectores donde se han detectado un mayor número de incidentes han sido el Sector Tributario y Financiero seguido del Sector Transporte y Sector Energía.

Además, en el marco de la pandemia los ataques informáticos han aumentado considerablemente. Los ciberdelincuentes han aprovechado la confusión que genera la COVID-19 para provocar interrupciones en los sistemas sanitarios[21] e incluso en actividad administrativa[22].

Dada la importancia y las consecuencias que este tipo de ataques tienen para la actividad diaria, este trabajo de fin de grado se centrará en analizar el marco legal de los daños y sabotajes informáticos recogidos en los artículos 264 y 264 bis CP haciendo especial

[21] Publicación en el periódico El País: «El hospital Moisès Broggi, víctima de un ataque informático en plena pandemia» 3 de septiembre de 2020. https://elpais.com/espana/catalunya/2020-09-03/el-hospital-moises-broggi-victima-de-un-ataque-informatico-en-plena-pandemia.html

[22] Publicación en el periódico El País: «El sistema informático del SEPE sufre un ciberataque» 9 de marzo de 2021. https://elpais.com/economia/2021-03-09/el-sistema-informatico-del-sepe-sufre-un-ciberataque.html

referencia a las novedades que introdujo la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de daños informáticos.

Antes de ello, y en aras de conocer el contexto normativo de estas actuaciones, realizaremos una aproximación a la normativa internacional, europea y finalmente española de los delitos informáticos.

IV. REGULACIÓN INTERNACIONAL, EUROPEA Y ESPAÑOLA

A nivel internacional, los delitos informáticos generan una gran preocupación dada la grave repercusión que pueden tener en el desarrollo económico y funcional de las empresas. En este sentido, la OCDE declara que los ciberataques pueden causar catástrofes semejantes a pandemias o terremotos, e incluso generar un colapso global[23]. Esta preocupación se refleja en la distinta normativa, ya sea internacional, europea o incluso española.

1. MARCO INTERNACIONAL

Desde una perspectiva internacional, la preocupación por la ciberseguridad se remonta al año 1997 con la emisión por el Grupo de los ocho países más industrializados económicamente del planeta[24] de un comunicado relativo a las acciones y principios para combatir la cibercriminalidad. Posteriormente, en 1990, la Asamblea General de las Naciones Unidas adoptó una resolución que versaba sobre la legislación de delitos informáticos. La Unión Internacional de Telecomunicaciones publicó tras la Cumbre Mundial sobre la Sociedad de la Información de 2003, la Declaración de Principios de Ginebra y el Plan de Acción de Ginebra donde destaca la importancia que se otorga a las medidas contra la ciberdelincuencia.

Asimismo, debemos destacar la Unión Internacional de Telecomunicación (UIT) de las Naciones Unidas que, en 2007 puso en marcha la Agenda Global para la Ciberseguridad con

[23] SOMMER, P y BROWN, I.: OCDE «Reducing Systemic Cybersecurity Risk», *OECD project "Future Global Shocks"*, 2011, accesible en https://www.oecd.org/gov/risk/46889922.pdf

[24] Grupo de los Ocho (G8) al que pertenecen Gran Bretaña, Rusia, Francia, Italia, Japón, Alemania y Canadá.

el objetivo de crear un marco de cooperación internacional para mejorar la seguridad en internet. Posteriormente, se llevó a cabo la Declaración de Seúl para el futuro del Internet[25] donde se contemplan medidas para la reducción de la actividad ilícita en internet.

En el contexto actual cabe destacar el Convenio sobre la Ciberdelincuencia, sancionado en Budapest en 2001. Se trata de un acuerdo internacional cuyo objetivo es establecer una serie de herramientas legales para «proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional»[26]. En particular, aborda las infracciones relacionadas con el acceso ilegítimo a la totalidad o parte de sistemas informáticos, interceptación por medios técnicos de datos informáticos, comisión de actos que dañen o deterioren datos informáticos, obstaculización del funcionamiento de sistemas informáticos, abuso de dispositivos y, por último, la falsificación informática.

Así, el documento tiene cuatro capítulos en los que, partiendo de definiciones consensuadas por todas las partes, se clasifican las infracciones en cuatro categorías:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Comprendiendo delitos como el acceso e intercepción ilícita, la interferencia de datos o el abuso de dispositivos.

2. Delitos informáticos. Entendidos estos como la introducción, alteración, borrado o supresión de datos informáticos.

3. Delitos relacionados con el contenido. Como, por ejemplo, los relacionados con la pornografía infantil.

4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Posteriormente, se insta a los países adheridos a tipificar en su derecho interno dichas figuras articulando a su vez las distintas medidas de cooperación internacional entre las que encontramos: designación de un punto de contacto disponible las veinticuatro horas del día,

[25] Declaración de Seúl. Conferencia Ministerial de la OECD sobre el futuro de la economía en Internet. Seúl, junio 2008.

[26] Preámbulo Párrafo 4, Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia.

los siete días de la semana para la localización de sospechosos, recolección o envío de evidencia digital.

A día de hoy se trata de un convenio internacional ya que se han adherido más de 56 países, entre los que encontramos Estados Unidos, México, Argentina y todos los pertenecientes a la Unión Europea.

Fuera de las conferencias internacionales, todos los países han ido modificando sus textos legales para adaptarse a la evolución de las nuevas tecnologías, sin embargo, en este punto haremos hincapié en la primera regulación sobre la materia que, como veremos, es muy temprana.

En un primer grupo, mencionaremos los países que decidieron desarrollar leyes específicas en torno a la ciberseguridad. Dentro este grupo se incluyen países como Francia, Gran Bretaña, Irlanda o Estados Unidos. Así, Francia desarrolló el derecho informático por primera vez en la Ley n.º 78-15 relativa a la informática, ficheros y libertades[27]. Actualmente, cuenta con más de diecisiete textos legales que profundizan en el mencionado derecho informático y que modifican esta ley. Por su parte, Gran Bretaña promulgó en 1990 la Computer Misuse[28] en la que ya tipificaba determinados delitos informáticos, si bien no definía qué podía entenderse por informático. Irlanda desarrolló en 1991 el Criminal Damages Act mientras que Estados Unidos adoptó el Computer Fraud and Abuse Act en el año 1986.

Por otro lado, encontramos países que decidieron incluir la regulación sobre delitos informáticos dentro del propio Código Penal. Dentro de este grupo se encuentran países como España, Alemania, Suecia, Dinamarca o Panamá.

2. DELITOS INFORMÁTICOS EN EL SENO DE LA UNIÓN EUROPEA

En el seno de la UE cabe destacar 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 y

[27] Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[28] Computer Misuse Act 1990.

por la que se sustituye la Decisión marco 2005/222/JAI del Consejo[29]. Este texto cita entre sus objetivos la aproximación de las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información, mediante el establecimiento de normas mínimas referidas a la definición de las infracciones penales y las sanciones aplicables, así como mejorar la cooperación entre las distintas autoridades competentes[30]. En el texto se insta a los Estados miembros a sancionar como infracción penal el acceso sin autorización a los sistemas de información (art. 3), la obstaculización o interrupción significativas del funcionamiento de un sistema de información (art. 4), borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información en los casos que no sean de menor gravedad (art. 5), así como la interceptación, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información sin autorización (art. 6).

Como parte del desarrollo del citado Convenio de Budapest, la Unión Europea cuenta con la Agencia de Ciberseguridad Europea (ENISA[31]) que se encargar de garantizar la ciberseguridad, ciberresiliencia y confianza dentro de la Unión. Sus funciones se centran en la asistencia a los distintos Estados miembros a la hora de incorporar, aplicar o elaborar políticas de ciberseguridad.

Además, desarrolló en 2016 la Directiva sobre Seguridad de las Redes y de los Sistemas de Información (Directiva NIS[32]). Esta directiva se encuentra en revisión debido a las limitaciones que mostró ante la pandemia COVID-19; por ello, se ha presentado y está en desarrollo la Directiva NIS2. Actualmente está vigente el programa Horizonte Europa, un programa marco que subvenciona proyectos de investigación tecnológica entre los que se encuentran los relacionados con la seguridad digital.

[29] Véase más ampliamente sobre toda la normativa europea, GIL GIL, A./HERNÁNDEZ BERLINCHES, R. (Coords.), *Cibercriminalidad, cit.*, pp. 174-176.

[30] También en la doctrina se pone de relieve la necesidad de crear una legislación penal y procesal que pueda desarrollarse en un conjunto de Estados como medio de poder hacer frente a este tipo de criminalidad. La armonización no debería limitarse al ámbito sustantivo sino también a las medidas referidas a la investigación y enjuiciamiento criminal. En este sentido, véase, por ejemplo, BORJA JIMÉNEZ, E., *Curso de Política Criminal*, 3.ª ed., Tirant lo Blanch, Valencia, 2021, pp. 323-324.

[31] European Union Agency for Network and Information Security.

[32] Directiva (UE) 2016/1148 Del Parlamento Europeo y del Consejo de 6 de Julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

En la resolución del Parlamento europeo, de 3 de octubre de 2017, sobre la lucha contra la ciberdelincuencia (2017/2068(INI)) se subraya que la lucha contra la ciberdelincuencia debe consistir, ante todo, en proteger y reforzar las infraestructuras críticas y otros dispositivos conectados a la red y no solo en ejecutar medidas represivas. Además, considera que es necesario racionalizar las definiciones comunes de ciberdelincuencia, guerra cibernética, ciberseguridad, acoso cibernético y ciberataque, con el fin de garantizar una definición jurídica común que compartan las instituciones y los Estados miembros de la Unión. Asimismo, reitera la importancia de las medidas jurídicas tomadas a nivel europeo con objeto de armonizar la definición de los delitos relacionados con ataques contra sistemas de información, así como con la explotación sexual de menores en línea, y obligar a los Estados miembros a establecer un sistema para el registro, la producción y la puesta a disposición de datos estadísticos sobre estos delitos a fin de combatirlos con mayor eficacia.

Las líneas de actuación que propone se articulan en torno a seis ámbitos: prevención, aumentar la responsabilidad de los prestadores de servicios, reforzar la cooperación policial y judicial, prueba electrónica, creación de capacidades a nivel europeo, cooperación mejorada con terceros países.

Cabe citar por último el Reglamento (UE) 2019/796 del Consejo de la Unión Europea, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros. Para que un ciberataque se encuadre dentro de su ámbito de aplicación, debe considerarse:

a) Una amenaza externa, es decir, que: «a) se originen, o se cometan, desde el exterior de la Unión; b) utilicen infraestructura fuera de la Unión; c) hayan sido cometidos por una persona física o jurídica, una entidad o un organismo establecidos o que tengan actividad fuera de la Unión; o d) hayan sido cometidos con el apoyo, bajo la dirección o bajo el control de una persona física o jurídica que tenga actividad fuera de la Unión.»

b) Que suponga una de las siguientes acciones, «cuando no estén debidamente autorizadas por el propietario o por otro titular de derechos del sistema o de los datos, o de parte de los mismos, o no estén permitidas por el Derecho de la Unión o de un Estado miembro: acceso a

sistemas de información; intromisión en sistemas de información; intromisión en datos; o interceptación de datos».

3. REGULACIÓN ESPAÑOLA SOBRE CIBERDELINCUENCIA

España ratificó el Convenio sobre la Ciberdelincuencia de Budapest el 1 de octubre de 2010 y, como miembro de la Unión Europea, traspone sus directivas en el ordenamiento jurídico. Ahora bien, tal y como hemos visto al comienzo de este trabajo, el Código Penal español no contiene un capítulo concreto en el que recoja delitos cuyo bien jurídico protegido sea la seguridad en los sistemas informáticos. Sin embargo, más allá de lo previsto en dicho texto normativo, España cuenta con otras normas relacionadas con la ciberseguridad, entre las que encontramos: Ley 36/2015, de 28 de septiembre, de Seguridad Nacional; Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana o la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Si atendemos a las previsiones del Código Penal se observa que la regulación de comportamientos delictivos relacionados con el ciberespacio está dispersa en distintos títulos. Siguiendo a VELASCO NUÑEZ[33] podemos agruparlos de la siguiente forma:

1) Delitos cibereconómicos: estafa (art. 248.2 CP), defraudación (art. 255 CP) , hurto de tiempo (art. 256 CP), daños informáticos, denegación de servicio, virus informáticos (art. 264 CP), contra la propiedad intelectual e industrial (art. 270 CP); espionaje informático (art. 278 CP); falsedades (art. 390 CP); blanqueo de capitales (art. 301 CP; difusión de datos económicos engañosos para alterar el precio de instrumento financiero o contrato de contado sobre materias primas (art. 284. 1.2º CP).

2) Ciberintrusivos: Pornografía infantil (art. 189 CP); abuso sexual (art. 183 bis CP); *Child grooming* (art. 183 ter CP); *stalking* (art. 172 ter CP); quebrantamiento de alejamiento (art. 468.3 CP); descubrimiento y revelación de secretos. *Hacking* (arts. 197 y ss. CP); calumnias e injurias (arts. 205,208 CP); amenazas coacciones y extorsiones (art.

[33] VELASCO NÚÑEZ, E./SANCHÍS CRESPO, C., *Delincuencia informática. Tipos delictivos e investigación con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, Valencia, 2019, pp. 27 y ss.

169/172/243 CP; infidelidad en la custodia de documentos y violación de secretos para su venta (arts. 417-423 CP); suplantación y robo de la personalidad; contra el orden público (arts. 559-560 CP); incitación al odio y a la violencia contra grupos/diferentes (art. 510 CP)

3) Ciberterrorismo: conductas de los arts. 573.2 y 573 bis CP; conductas del art. 575.2 CP; conductas del art. 578 CP; conductas del art. 579 CP[34].

Cabe señalar que en el debate doctrinal se plantea si estas figuras delictivas protegen nuevos bienes jurídicos o si en realidad estamos ante nuevas formas de comisión de los delitos tradicionales. En relación con la cibercriminalidad en sentido estricto (las conductas de intrusismo informático recogidas en el art. 197 bis dentro de los delitos contra la intimidad y los daños informáticos recogidos dentro de los delitos contra el patrimonio) parte de la doctrina jurídica entiende que es necesaria la definición de un nuevo bien jurídico que dote a los delitos informáticos de autonomía propia, ya que la regulación actual genera numerosos problemas de interpretación[35]. Este bien jurídico se identificaría con la «seguridad informática»[36]. En base a esta argumentación, dichos autores plantean el traslado de los delitos informáticos a un nuevo título que agrupe todas las figuras delictivas que vulneran dicho bien jurídico.

Sin embargo juristas como GONZÁLEZ RUS[37] defienden que la aparición de nuevos objetos materiales no justifica la creación de nuevos bienes jurídicos. En este sentido actúa el legislador español a la hora de incluir los delitos informáticos en diferentes títulos, entiende que el bien jurídico protegido en cada caso se corresponde con el de la naturaleza de infracción cometida.

[34] Véase también una relación de los delitos y nuevas formas comisivas por el uso de las TIC en GIL GIL, A./HERNÁNDEZ BERLINCHES, R., *Cibercriminalidad, cit.*, pp. 178-179.

[35] GIL GIL, A./HERNÁNDEZ BERLINCHES, R. (Coords.), *Cibercriminalidad, cit.*, p. 214. También, DE LA MATA BARRANCO, N., HERNÁNDEZ DÍAZ, L: «El delito de daños informáticos: una tipificación defectuosa» en *Estudios Penales y Criminológicos*, vol. XXIX, Servizo de Publicacións da Universidade de Santiago de Compostela, 2009, pp. 324 y ss.

[36] GIL GIL A., «Daños informáticos», en SANZ DELGADO, E. y FERNÁNDEZ BERMEJO, D., *cit.*, p. 468.

[37] GONZÁLEZ RUS, J. J., «Precisiones conceptuales y político-criminales sobre la intervención penal en internet», en *Delito e Informática: algunos aspectos (Cuadernos Penales José María Lidón, n.º 4)* Universidad de Deusto, 2007, p. 30.

Frente a este debate existen posturas intermedias[38] que sostienen que cuando la acción ilícita recaiga sobre datos, programas o sistemas informáticos propiamente dichos, se podría argumentar la creación de un nuevo bien jurídico protegido. Sin embargo, si la conducta típica se basa en los medios utilizados, entonces el bien jurídico protegido será el de la naturaleza de la infracción cometida.

De todas formas, aunque este debate siga abierto, actualmente España no cuenta con un capítulo específico relativo a los delitos informáticos y por ello, su estudio resulta complicado. En el siguiente apartado trataremos de estudiar el contexto y marco jurídico de los daños y sabotajes informáticos, actividades ilícitas de gran actualidad.

V. DAÑOS INFORMÁTICOS O SABOTAJE INFORMÁTICO

Tal y como hemos anunciado al comienzo de esta exposición, la aparición de conductas delictivas relacionadas con las TIC está ligada al desarrollo de las propias herramientas de información. Con ello, el ciberespacio y más concretamente Internet, se enfrentan a graves problemas de falta de regulación debido a la propia rapidez de desarrollo de las técnicas informáticas. Sin embargo, en España el problema no se remite al rápido desarrollo de las TICs, sino a la fórmula empleada para abarcar todas las conductas que podrían representar un delito informático.

Ya en 1995 el Código Penal incorporó en el artículo 264 una modalidad agravada de daños en cosa ajena. Este precepto castigaba a quien «destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos». Se da, por tanto, una primera aproximación hacia los delitos informáticos. Sin embargo, parte de la doctrina entendía que el legislador no había sido capaz de abarcar todas las posibles conductas relativas a los daños informáticos y

[38] En este sentido BUENO ARÚS, F., «El delito informático», *Actualidad Informática Aranzadi,* n.º 11, 1994, p. 2 y ROMEO CASABONA, C. M.ª, *Poder Informático y Seguridad Jurídica,* Fundesco, 1987, pp. 42-43.

que, dada su importancia, merecían una regulación expresa[39]. Como ya hemos visto, este debate sigue todavía presente sin que se haya llegado a un acuerdo en la doctrina jurídica.

Más de una década después, y en el seno de la Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, el legislador español amplió la regulación existente e incluyó a través de la Ley Orgánica 5/2010, de 22 de junio, una regulación sobre la materia distinguiendo dos conductas punibles diferenciadas:

- La primera, relativa a los daños y que, además de lo incluido inicialmente en el CP de 1995, incluía la obstaculización o interrupción de sistemas informáticos ajenos. Así, en esta nueva tipificación se incluyeron multitud de intromisiones que interfiriesen tanto en datos o programas informáticos, como en sistemas informáticos completos.
- La segunda estaba referida a la revelación de secretos, comprendiendo el acceso sin autorización «vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o parte del mismo»[40].

Tal y como expresa GIL GIL[41] el legislador en lugar de tratar la ciberseguridad como bien jurídico independiente, se centra en la protección de los bienes jurídicos a los que una falla de ciberseguridad podría afectar.

Posteriormente, a través de la LO 1/2015 introduce en el Capítulo IX, dedicado a los daños, dentro del Título XIII «Delitos contra el patrimonio y contra el orden socioeconómico» una serie de delitos informáticos que pretenden ofrecer a los datos y sistemas informáticos la misma protección que a los objetos físicos. Así se modifica el art. 264 y se añade el art. 264 bis. Según indica la exposición de motivos: «Se regulan separadamente, de un modo que permite ofrecer diferentes niveles de respuesta a la diferente

[39] CORCOY BIDASOLO, M., «Protección penal del sabotaje informático: especial consideración de los delitos de daños» en MIR PUIG, S. (Coord.), *Delincuencia informática,* Barcelona, 1992, p. 145. También en DE LA MATA BARRANCO, N./HERNÁNDEZ DÍAS, L., «El delito de daños informáticos: una tipificación defectuosa», *cit.*, p. 311.

[40] Exposición de Motivos XIV de Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

[41] GIL GIL A., «Daños informáticos» en SANZ DELGADO, E. y FERNÁNDEZ BERMEJO, D. (Coords.) *Tratado de Delincuencia Cibernética,* Navarra, Aranzadi, 2021, p. 467.

gravedad de los hechos, los supuestos de daños informáticos y las interferencias en los sistemas de información». Entre las novedades cabe destacar la inclusión de una agravante cuando el objetivo del ataque va referido a infraestructuras críticas. Además en el art. 264 ter se castigan como actos preparatorios la producción, la adquisición para su uso, la importación o la facilitación a terceros, de cualquier modo, con la intención de cometer alguno de los delitos a que se refieren los arts. 264 y 264 bis, de: 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. Este precepto tiene carácter novedoso y trata de dar cumplimiento a los previsto en el art. 7 de la Directiva 2013/40/UE.

Si bien los arts. 264 y 264 bis serán estudiados a continuación, es necesario hacer un breve inciso poniendo de relieve algunas conductas que podrían encajar en los mismos. Como ya hemos visto, el hecho de que nos encontremos en una sociedad cada vez más globalizada y el consecuente desarrollo del ciberespacio ha generado un nuevo ámbito delictivo en el que cada día se observan nuevas actuaciones ilícitas[42]. A modo de ejemplo:

- Malware

La distribución de malware se caracteriza por la infección de un virus destructivo en un sistema informático con el objetivo de dañar, controlar o modificar los datos que contiene[43]. Dentro de los malware existen subcategorías como los gusanos (*worms*) o los troyanos (*trojans*) según el tipo de virus que se inserte en el equipo. Muestra de la importancia de este tipo de conductas fue la infección en el año 2017 de equipos informáticos de empresas de todo el mundo entre los que se encuentra Telefónica, el sistema británico de salud y la red ferroviaria alemana. A través del gusano «WannaCry» se cifraban los archivos del sistema

[42] DE LA MATA BARRANCO, N., «Los delitos contra la integridad y disponibilidad de datos y sistemas informáticos después de la LO 1/2015» en BACIGALUPO, FEIJOO, ECHANO (Coords.), *Estudios de Derecho Penal: homenaje al profesor Miguel Bajo,* Ed. Universitaria Ramón Areces, 2016, p.1090. También VELASCO NÚÑEZ, E./SANCHÍS CRESPO, C., *Delincuencia informática*, *cit.,* p. 52.

[43] MIRÓ LLINARES, F., *El cibercrimen*, *cit.*, p. 59.

infectado impidiendo realizar cualquier operación con él. Esta infección estuvo descontrolada cuatro días y se estima que causó 3.000 millones de euros en daños[44].

- Insiders

Estos ataques son realizados por personas que trabajan o trabajaban en la empresa afectada y aprovechan su posición para destruir o dañar la mayor cantidad posible de información. Según datos extraídos del estudio «2020 Cost of Insider Threats Global Report»[45] desde el año 2018 este tipo de ataques han sufrido un crecimiento de más del 30%. Como ejemplo en nuestro país encontramos la reciente sentencia n.º 358/2022 del Tribunal Supremo, de 7 de abril, que analizaremos más adelante.

- Ataques DoS y DDoS

La inutilización de los sistemas informáticos por sí misma, puede generar una pérdida en sentido económico y es por ello que se entienden comprendidos dentro de las nuevas conductas informáticas delictivas los ataques DoS (ataques de denegación de servicios), DDoS (ataques distribuidos de denegación de servicios). El último gran ataque recibido en España fue en el mes de marzo de 2022 cuando la web del Congreso de los Diputados estuvo inactiva durante 45 minutos. El ataque se fundamentó en el acceso simultáneo por parte de numerosos equipos informáticos que inhabilitaron el acceso a la web al colapsar el servidor[46].

Una vez contamos con una perspectiva práctica de lo que suponen los daños y el sabotaje informáticos, pasamos a estudiar el alcance jurídico de estas actividades ilícitas. Ya sabemos que en la regulación vigente podemos identificar dos actuaciones: en primer lugar, aquellas acciones que se realizan sobre el propio sistema informático ya sea dañando, alterando o suprimiendo datos y, por otro lado, las ejecutadas para la obstaculización o interrupción del

[44] «Cinco años de WannaCry, el ciberataque mundial con armas de la NSA», accesible en https://www.eldiario.es/tecnologia/cinco-anos-wannacry-ciberataque-mundial-armas-nsa_1_8983773.html

[45] «2020 Cost of Insider Threats Global Report» realizado por Ponemon, accessible en https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/UK-VR-Proofpoint-Report-2020-Cost-of-Insider-Threats.pdf

[46] «El Congreso sufre el modelo de ciberataque más utilizado desde Rusia» accesible desde https://www.vozpopuli.com/tecnologia/web-congreso-ciberataque-rusia.html?utm_medium=Social&utm_source=Twitter#Echobox=1648124808

funcionamiento del sistema informático[47]. Ambas aparecen reguladas en el artículo 264 y 264 bis CP, respectivamente, y la aplicación de una u otra figura típica «vendría determinada por la capacidad de la acción para afectar a la operatividad o al funcionamiento del sistema informático en su conjunto»[48].

El Anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información, define los sabotajes junto al terrorismo y al vandalismo como los ataques implementados con el objetivo de interrumpir o degradar la prestación de un servicio, «provocando daños relevantes en la continuidad del servicio de una institución». Hay que tener en cuenta que el artículo 573 ter CP califica como terrorismo a las actividades de los artículos 264 y 264 bis CP (junto a las de los arts. 197 bis y 197 ter) que se realicen con alguna de las siguientes finalidades: 1.ª Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o abstenerse de hacerlo. 2.ª Alterar gravemente la paz pública. 3.ª Desestabilizar gravemente el funcionamiento de una organización internacional. 4.ª Provocar un estado de terror en la población o en una parte de ella.

Debido a la restricción de espacio que este trabajo conlleva, realizaremos una aproximación de las cuestiones comunes a los dos preceptos y en un segundo punto, estudiaremos las acciones típicas concretas de los artículos 264 y 264 bis CP.

[47] MIRÓ LLINARES, F., *El cibercrimen*, *cit*, p. 58. Véase también NAVARRO FRÍAS, I., «Delitos contra el patrimonio y el orden socioeconómico II. Defraudaciones, insolvencias punibles, alteración de precios en concurso y subastas públicas y daños», en ROMEO CASABONA/SOLA RECHE/BOLDOVA PASAMAR (Coords.) *Derecho penal. Parte especial*, 2.ª ed., Comares, Granada, 2022, p. 406, quien destaca que en el art. 264 bis la actuación sobre los datos, programas o documentos concretos tiene relevancia en cuanto es un medio de afectar al sistema, pues la conducta se dirige contra los sistemas en su totalidad.

[48] Circular 3/2017 de la FGE de 21 de septiembre, sobre la reforma del código penal operada por LO 1/2015, de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos, p. 30. Consultar en https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2017-00003.pdf

1. CUESTIONES COMUNES A LAS DISPOSICIONES 264 Y 264 BIS CP

1.1. Bien jurídico protegido

Ya hemos visto anteriormente que en la actualidad existe un debate sobre si cabe hablar de un nuevo bien jurídico en relación con los ciberdelitos en sentido estricto. En los daños y sabotaje informáticos, este debate se centra, por un lado, en una defensa de que los artículos 264 y 264 bis CP se encuadran en los daños comunes y que, por tanto, el bien jurídico protegido sería el patrimonio individual; o si, por el contrario, es posible identificar un bien jurídico diferente.

GIL GIL[49] expresa su disconformidad con el punto de vista actual del legislador español puesto que, en sus propias palabras, «el legislador desconoce la problemática actual de la ciberdelincuencia, sus efectos propios y la importancia de la ciberseguridad como bien jurídico independiente», entendiendo que los delitos informáticos protegen un bien jurídico colectivo más amplio que el patrimonial, pues los daños realizados van más allá de un daño patrimonial ya que afectan a la integridad y disponibilidad de los propios sistemas informáticos. Además, RUEDA MARTÍN[50] añade que los ataques a los sistemas informáticos pueden ser «individuales o colectivos, plurales y variados» y que, por tanto, el bien jurídico protegido no se puede reducir al patrimonio individual, ya que hacerlo supondría excluir ciertos comportamientos que deben ser atendidos.

[49] GIL GIL A., «Daños informáticos», en SANZ DELGADO, E. y FERNÁNDEZ BERMEJO, D., *cit.,* p. 470. También en esta línea cabe citar a CARRASCO ANDRINO, M.ª del M., «Lección 23ª. Descubrimiento y revelación de secretos» en ÁLVAREZ GARCÍA (Director) y MANJÓN-CABEZA y VENTURA PÜSCHEL (Coords.), *Derecho penal español, Parte Especial (I)* 2.ª ed., Tirant lo Blanch, 2011, p. 783. Esta autora defiende que a través de estos artículos se protege «la indemnidad de los sistemas informáticos como contenedores de información sensible y de los que dependen, además, las infraestructuras y los servicios electrónicos en la nueva Sociedad de la Información». Asimismo, MORÓN LERMA, E., *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red,* Aranzadi, 2002, p. 85 expresa que nos encontramos ante un nuevo «valor social, un interés de nuevo cuño, cifrado en la seguridad de los sistemas informáticos, o en la seguridad informática, o en la seguridad en el funcionamiento de dichos sistemas informáticos» que merece protección individual.

[50] RUEDA MARTÍN, M.ª A., «La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español»*, Diritto Penale Contemporaneo,* 2020, pp. 203-204.

En suma, podríamos decir que los defensores de esta postura[51] interpretan que el bien jurídico protegido de los delitos informáticos es la ciberseguridad, esto es, la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos[52], o expresado en otras palabras, la «seguridad informática»[53]. Este objeto de protección se encuentra recogido en el propio preámbulo del Convenio de Budapest donde se expresa que «el presente Convenio resulta necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos»[54]. De esta forma, analizando estos tres conceptos entendemos que dentro de la seguridad informática se encuentra «la confidencialidad», es decir, la propiedad de la información sin que sea accesible a individuos no autorizados; «la integridad» de los datos, entendiéndose la exactitud y la no alteración de los mismos; y por último «la disponibilidad», es decir, el almacenamiento correcto de datos. Con todo, se puede interpretar que dentro del bien jurídico aludido no solo se protegería la información contenida, sino también el buen funcionamiento de los sistemas informáticos[55].

En base a esta argumentación, dichos autores plantean el traslado de los delitos informáticos a un nuevo título que agrupe todas las figuras delictivas que vulneran alguno de los conceptos aludidos. En este sentido, QUINTERO OLIVARES[56] manifiesta que la regulación actual es «farragosa» y defiende que los delitos informáticos deberían estar recogidos en un título independiente al del delito común de daños.

---

[51] DE LA MATA BARRANCO, N., «La tipificación de los denominados "Derechos informáticos"», *Revista de Derecho Penal,* n.º 26, 2018, pp. 257 y ss., junto a LEYRE HERNÁNDEZ DÍAZ, L. *cit.*, pp. 324 y ss.; SÁNCHEZ MAGRO, A., «El ciberdelito y sus implicaciones procesales» en GARCÍA MEXÍA P., *Principios de Derecho de Internet*, 2.ª ed., Tirant lo Blanch, Valencia, 2005, pp. 306 y ss.; GIL GIL, A./HERNÁNDEZ BERLINCHES, R. *Cibercriminalidad, cit.*, pp. 148 y ss.; GUTIÉRREZ FRANCÉS, M. L., «Intrusismo informático (hacking). ¿Represión penal autónoma?», *Informática y Derecho,* n.º 12-15, 1994, p. 1177.

[52] Principios básicos de la seguridad de la información según el modelo CIA (por sus siglas en inglés; Confidentiality, Integrity and Availability). Modelo a través del cual se diseñan las políticas de seguridad cibernética en el ámbito de la seguridad de la información.

[53] GIL GIL A., «Daños informáticos», en SANZ DELGADO, E. y FERNÁNDEZ BERMEJO, D., *cit.,* p. 468.

[54] Convenio del Consejo de Europa sobre Cibercriminalidad, Budapest, 23 de noviembre de 2001.

[55] GIL GIL A., «Daños informáticos», en SANZ DELGADO, E. y FERNÁNDEZ BERMEJO, D., *cit.,* p. 469.

[56] QUINTERO OLIVARES, G., «Art. 264», en QUINTERO OLIVARES (Dir.)/MORALES PRATS (Coord.), *Comentarios a la Parte Especial del Derecho penal*, 10.ª ed., Aranzadi, Pamplona, 2016, p. 751.

En el extremo contrario, juristas como GONZÁLEZ RUS[57], consideran que la aparición de nuevos objetos materiales no justifica la creación de nuevos bienes jurídicos y que, por lo tanto, nos encontramos ante tipos específicos y/o agravados de daños comunes[58]. También, PUENTE ABA[59], entre otros[60], se refiere a este asunto manifestando su posición en contra de la configuración de bien jurídico autónomo de los daños informáticos basándose en los principios de mínima intervención del Derecho penal y proporcionalidad[61].

Por su parte la jurisprudencia se ha pronunciado defendiendo que el bien jurídico protegido por los daños informáticos recogidos en el artículo 264 CP: «constituye una figura concretada en la destrucción o menoscabo material o funcional de la propiedad ajena, de manera que el objeto de ajeno dominio sobre el que se lleva a cabo la acción resulte destruido o menoscabado, sea en su entidad física sea en la funcionalidad que le es propia. La acción de destruir, alterar, inutilizar, dañar de cualquier otro modo datos programas o documentos electrónicos contenidos en un soporte informático, venía a comportar un daño patrimonial por reparación o sustitución del objeto material sobre el que habían operado dichas acciones»[62]. Considera por tanto que los daños informáticos protegen el patrimonio, un bien jurídico individual.

Una vez comprendidas todas las posturas, en este trabajo se va a seguir el criterio de que, a pesar de su incorrecta ubicación, los delitos de daños informáticos protegen un bien jurídico más amplio que el patrimonio ya que, como veremos, el objeto material de estos

[57] GONZÁLEZ RUS, J. J., «Precisiones conceptuales y político-criminales sobre la intervención penal en internet», en *Delito e Informática: algunos aspectos (Cuadernos Penales José María Lidón, n.º 4)* Universidad de Deusto, 2007, p. 30.

[58] RODRÍGUEZ MESA, M.ª J., *Los delitos de daños, capítulo IX del título XIII del CP tras la reforma de la LO 1/2015, cit.*, p. 61.

[59] PUENTE ABA, L. M., «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿Debe protegerse de forma autónoma la seguridad informática?», en FARALDO CABANA, P. y PUENTE ABA, L. M., *Nuevos retos del derecho penal en la era de la globalización,* Tirant lo Blanch 2004, pp. 398 y ss.

[60] MESTRE DELGADO, E., «Tema 13. Delitos contra el patrimonio y contra el orden socioeconómico», en LAMARCA PÉREZ (Coord.), *Delitos, La parte especial del Derecho Penal,* Dykinson, Madrid, 2019, pp. 342-343. TRAPERO BARREALES, P., «Algunas consideraciones en torno al bien jurídico protegido en el delito de daños informáticos», en PAREDES CASTAÑÓN y otros (Dir.) *Libro homenaje al profesor Diego-Manuel Luzón Peña con motivo de su 70º aniversario, vol. II*, Ed. Reus, 2020, p. 1948, considera que el bien jurídico protegido en estos delitos es el patrimonio, ahora bien, entendido desde el valor funcional de los datos y sistemas informáticos.

[61] PUENTE ABA, L. M. , «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿Debe protegerse de forma autónoma la seguridad informática?», *cit.,* pp. 398 y ss.

[62] Sentencia del Juzgado de lo Penal de Gijón, de 06 de julio de 2016 (ECLI: ES:JP:2016:39).

delitos son los equipos informáticos, también denominados, de software. El software abarca todo lo intangible ya que tiene una naturaleza binaria, que a partir de 0s y 1s codifica los datos[63]; por tanto, no podemos tratar estos delitos desde el concepto tradicional de «daños», sino que debemos ampliar el espectro, entendiendo que el bien jurídico protegido en estos casos es, como dice la Convención de Budapest, «la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos».

1.2. Ajenidad del objeto material

Un elemento común a los daños y sabotaje informáticos es que los datos o el sistema al que se ha tenido acceso deben ser ajenos de tal forma que pertenezcan o sean propiedad de otra persona. La propiedad debe determinarse según la normativa civil de propiedad intelectual[64]; si bien, al encontrarnos ante elementos inmateriales, existe una latente dificultad para determinarla[65]. Como indica RODRÍGUEZ MESA se trata de una cuestión complicada en este ámbito ya que es posible que el titular del software y el titular de hardware sean distintos o que haya derechos de distintos titulares sobre el mismo objeto material. En este sentido, cita como ejemplo el ámbito de la empresa donde habrá que establecer hasta qué punto los datos, programas informáticos o documentos electrónicos contenidos en los ordenadores utilizados son propiedad de la empresa o del trabajador[66]. Es por ello que en aquellos casos en los que su determinación entrañe dificultades, la Fiscalía establece que la propiedad deberá interpretarse junto a la «falta de autorización», es decir, debe examinarse si el actor estaba habilitado para acceder a los datos dañados o alterados.

[63] RODRÍGUEZ MESA, M.ª J., *Los delitos de daños, capítulo IX del título XIII del CP tras la reforma de la LO 1/2015, cit.*, p. 62.

[64] MATA Y MARTÍN, R., «La tipificación de los denominados…», *cit.,* p. 67.

[65] Sobre la «ajenidad» véase el Auto Audiencia Provincial de Madrid (sección 4.ª de 3 de noviembre de 2017 en relación con la investigación por daños informáticos y encubrimiento relacionados con el borrado de los discos duros de ordenadores de un partido político. Un resumen de esta resolución puede consultarse en VELASCO NÚÑEZ, E./SANCHÍS PRIETO, C., *Delincuencia informática, cit.*, pp. 57 y ss.

[66] RODRÍGUEZ MESA, M.ª J., *Los delitos de daños, capítulo IX del título XIII del CP tras la reforma de la LO 1/2015, cit.*, p. 67.

2. DAÑOS, BORRADO O DETERIORO DE DATOS INFORMÁTICOS: ARTÍCULO 264 CP

El apartado 1 del artículo 264 CP tipifica el daño, borrado o deterioro de «datos informáticos, programas informáticos o documentos electrónicos ajenos» en cumplimiento del artículo 5 de la Directiva 2013/40/UE[67] denominado «interferencia ilegal en los datos».

2.1. Objeto material y acción típica

El objeto material está constituido por los datos, programas, ficheros o documentos electrónicos que componen el sistema informático, es decir, los elementos lógicos. Se trata, así, de un objeto inmaterial que puede ser denominado «flujo electromagnético»[68] pues incluye las órdenes e ideas registradas de forma electrónica. En consecuencia, los daños materiales constituirán la figura recogida en el artículo 263 CP mientras que, si los mismos daños se causan a datos recogidos en una infraestructura informática, estaremos frente a la acción típica de estudio. En este sentido, FLORES PRADA[69] establece que «quedarían fuera […] del campo de protección específica del art. 264 del Código Penal los daños contra elementos o componentes informáticos no ensamblados o montados (pantallas de ordenador, discos duros vírgenes, elementos de conexión, teclados, etc.), los daños contra elementos averiados y desechados, o los ataques contra elementos físicos que no afecten directamente al funcionamiento del sistema ni resulten esenciales para el mismo (ratón, altavoces, etc.), cuya tutela habría que remitir, en su caso, al tipo básico del art. 263 CP».

Desglosando el objeto material, por «datos» entendemos la representación de una información en un sistema informático, de tal forma que se puede encontrar conformada por letras y números e incluso por símbolos. Por otro lado, los «programas» son el conjunto de

[67] 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 y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Según el art. 5: «Los Estados miembros adoptarán las medidas necesarias para que borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad».

[68] ANDRÉS DOMÍNGUEZ, A. C., «Comentarios a los artículos 264, 264 bis, 264 ter y 264 quater», en GÓMEZ TOMILLO, M., *Comentarios prácticos al Código penal, Tomo III, Delitos contra el Patrimonio y socioeconómicos*, Aranzadi, Pamplona, 2015, p. 350.

[69] FLORES PRADA, I., *Criminalidad informática*, *cit.*, p. 173.

instrucciones y órdenes dadas a un sistema informático para cumplir una tarea específica. Los «ficheros electrónicos» son los medios electrónicos por los que se almacena la información. Por último, el «documento electrónico» constituye la información archivada en un soporte informático. Así, la acción típica debe recaer sobre alguno de los elementos a los que hemos hecho referencia.

Las acciones típicas descritas en el propio apartado primero del artículo 264 CP aparecen recogidas también en la Directiva Europea 2013/40/UE. De este modo, se castiga a quien atente a la integridad de los datos, interfiera ilegalmente en los mismos o borre, dañe, deteriore, altere, suprimiera o haga inaccesibles, «de manera grave y sin autorización». El art. 2 d) de la Directiva 2013/40/UE entiende como no autorizado todo aquel comportamiento, incluida la interferencia, «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».

Se trata de un delito de medios indeterminados que incluye desde el borrado manual hasta la infección del sistema con un virus informático que realice las mencionadas acciones. En la mayor parte de los casos, estos ataques se cometerán a través de las TIC sin que se ven afectados los dispositivos físicos, pues el objeto de estos delitos no son las herramientas, dispositivos o elementos externos (hardware) que se utilizan como soporte para operar informáticamente, sino la propia información, los bits, los programas, los elementos lógicos o de carácter inmaterial (software) de los sistemas de información[70]. No obstante, en opinión de la doctrina se podrían incluir en el tipo supuestos en los que el resultado típico se produce como consecuencia de la destrucción o deterioro del soporte físico receptor de los datos, programas o documentos electrónicos (hardware). En estos casos, puesto que el desvalor del delito de daños informáticos no implica el posible daño causado al objeto material receptor, habrá que apreciar un concurso medial entre este delito y el delito de daños tipificado en el art. 263 CP[71].

[70] TEJADA DE LA FUENTE, E., «La tipificación penal de los ataques a los sistemas de información», en CAMACHO VIZCAÍNO (Dir.), *Tratado de Derecho penal económico*, Tirant lo Blanch, Valencia, 2019, p. 919.

[71] En este sentido se pronuncia RODRÍGUEZ MESA, M.ª J., *Los delitos de daños, capítulo IX del título XIII del CP tras la reforma de la LO 1/2015, cit.*, p. 74.

Las conductas típicas pueden ser muy diversas pues comprende: borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles los datos o programas informáticos[72]. Atendiendo a la SAP Guipúzcoa (secc. 1ª) 120/2019 de 13 de junio (ECLI:ES:APSS:2019:708) «pueden ser sancionadas también aquellas conductas que a pesar de no causar un daño (por ejemplo, a través de su cancelación, supresión o deterioro), impiden al que tiene un legítimo derecho de disposición (propietario, posesor, etc.), acceder y utilizar de manera regular los datos y los programas informáticos».

Vemos que nos encontramos ante un daño que no tiene por qué ser cometido a través de comportamientos físicos, sino que se da con producirse un ataque al valor del objeto material[73], es decir, puede darse por un mero ataque funcional haciéndolos inoperativos o inaccesibles. Ahora bien, este debe ser grave y el resultado ocasionado debe ser, de misma manera, grave; es decir, nos encontramos ante un requisito de doble gravedad. La doctrina mayoritaria considera que «la exigencia de que la acción típica se realice de modo grave resulta redundante»[74] si bien entienden que a través de este requisito de doble gravedad el legislador ha tratado de dejar fuera aquellos resultados que generen mera incomodidad. Tal y como expresa FLORES PRADA se justifica en que «los sistemas digitales permiten con frecuencia la recuperación de datos y documentos electrónicos a través de procesos de restablecimiento o mediante el uso de copias de seguridad […] en cuyo caso el perjuicio se limita a meras molestias para el usuario que pueden carecer de relevancia penal»[75].

Así, dentro del artículo 264 CP tan solo se comprenderían aquellas conductas calificadas como graves. Si bien el precepto no establece los criterios para calificar a una conducta de grave, la Audiencia Provincial de Madrid en su sentencia n.º 23/2017, de 10 de enero (ECLI:ES:APM:2017:480) recoge una serie de reglas que pueden servir como base para la interpretación de la misma:

[72] Sobre el alcance de estos verbos véase, por ejemplo, TEJADA DE LA FUENTE, E., «La tipificación penal de los ataques a los sistemas de información», *cit.*, p. 917.

[73] ANDRÉS DOMÍNGUEZ, A. C., «Comentario al art. 264», *cit.*, p. 352.

[74] RODRÍGUEZ MESA, M.ª J., *Los delitos de daños, capítulo IX del título XIII del CP tras la reforma de la LO 1/2015, cit.*, p. 77. También MIRO LLINARÉS, F., «Delitos informáticos: Hacking. Daños» en ORTIZ DE URBINA (Coord.), *Memento Experto. Reforma Penal,* Ed. Ediciones Francis Lefebvre, 2010, p. 161.

[75] FLORES PRADA, I., *Criminalidad informática, cit.*, p. 180.

- Posibilidad de recuperación de datos informáticos
- Coste económico de la reparación del daño
- Complejidad técnica de la recuperación de los datos
- Duración de las tareas de recuperación
- Valor económico del perjuicio causado

En torno al concepto de gravedad, la doctrina propone que, junto al carácter económico, se tengan en cuenta otros como la imposibilidad de utilización temporal o definitiva o la aparición de una situación de desconfianza hacia el ofendido[76]. FLORES PRADA[77] por su parte entiende que dentro de las conductas graves se englobarían «los resultados irreparables como, por ejemplo, pérdidas definitivas de datos, ficheros o programas; alteraciones irreversibles, daños parciales o inutilizaciones sectoriales del sistema». En este sentido TEJADA DE LA FUENTE[78] expresa que para calificar una conducta como grave se deberán tener en cuenta criterios como la trascendencia e importancia de la alteración e incluso el perjuicio efectivo que haya supuesto para la victima la imposibilidad de disponer de determinada información durante el tiempo necesario para restaurar su funcionamiento.

Se ha planteado un problema particular en relación con los supuestos en que existen copias de seguridad. Las opiniones están divididas entre los que consideran que la consumación del delito requiere que desaparezcan de modo definitivo los datos (de modo que, si se destruyen los datos o programas informáticos, pero existen copias de seguridad habría que apreciar el delito en grado de tentativa) y aquellos otros autores para quienes el delito se consuma con el borrado, el daño, o la destrucción de esos datos al margen de si existen o no copias de seguridad. Eso no impide que esto último se tenga en cuenta a la hora de valorar la gravedad del delito[79].

[76] Así GONZÁLEZ HURTADO, J. A., *Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma,* Tesis doctoral inédita, Madrid, 2013, pp. 303-332.

[77] FLORES PRADA, I., *Criminalidad informática, cit.*, p. 180.

[78] TEJADA DE LA FUENTE, E., «La tipificación penal de los ataques a los sistemas de información», *cit.,* p. 921.

[79] Véase al respecto ANDRÉS DOMÍNGUEZ, A. C., «Comentario al art. 264 CP», *cit.*, pp. 354 y ss. defendiendo la segunda opción y también, con detalle, BALEA ROUCO, A., «Copias de seguridad, delito de daños informático y grado de ejecución», *Diario La Ley*, n.º 9939, Sección Doctrina de 25 de octubre de 2021,

2.2. Tipo subjetivo

En cuanto al elemento subjetivo del delito recogido en el artículo 264 CP, el dolo, conocimiento y voluntad de destruir, dañar o inutilizar los datos informáticos, programas o documentos electrónicos es suficiente. Ahora bien, se considera que cabe la posibilidad de que al mismo tiempo se realice la acción también con otras finalidades (por ejemplo, atentar contra la intimidad o atentar contra el patrimonio), de forma que cabrá acudir a las reglas del concurso de delitos[80].

2.3. Agravantes específicas

En este apartado expondremos las circunstancias agravantes específicas recogidas en el artículo 264 apartados 2 y 3 CP.

El apartado 2 prevé la imposición de «una pena de prisión de dos a cinco años y multa» cuando concurra alguna de las siguientes circunstancias: 1.º Se haya cometido en el seno de una organización criminal; 2.º se hayan generado daños de especial gravedad o afectado a un gran número de sistemas; 3.º haya ocasionado daños en sistemas de servicios públicos esenciales o afectado a bienes de primera necesidad; 4.º se haya creado una situación de grave peligro para la seguridad del «Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea»; o bien, 5.º se haya cometido empleando los medios descritos en el artículo 264 ter, siendo éstos programas informáticos especialmente creados para la comisión del delito descrito o una contraseña o código que permita acceder a todo o parte del sistema. También cuando los actos revistan extrema gravedad.

El apartado 3 por su parte, agrava la pena cuando la conducta se haya cometido mediante el uso ilícito de datos personales.

A continuación, se analiza el fundamento de estas agravaciones:

---

p. 3 donde indica que los tribunales también sostienen opiniones dispares pues mientras que algunos consideran que si existen copias de seguridad será un delito en grado de tentativa, en otras resoluciones se absuelve por falta de gravedad del resultado. En su opinión (p. 4) no hay que confundir el daño con el perjuicio: la gravedad del resultado (el daño) es distinta de la gravedad del perjuicio (el perjuicio determina la responsabilidad civil) y es con esto último con lo que hay que relacionar la existencia de copias de seguridad.

[80] QUINTERO OLIVARES, G., «Art. 264», en QUINTERO OLIVARES (Dir.)/MORALES PRATS (Coord.), *cit.,* p. 748.

1. *Comisión en el marco de una organización criminal*

La Directiva 2013/40/UE recoge en su artículo 9 la obligatoriedad por parte de los Estados de castigar con una «sanción máxima de privación de libertad de al menos cinco años cuando: a) se cometan en el contexto de una organización delictiva con arreglo a la Decisión marco 2008/841/JAI». Para entender lo establecido por «organización delictiva» debemos acudir al artículo 570 CP según el cual esta se define como el grupo estable y duradero formado por más de dos personas y que de forma coordinada se conciertan para cometer delitos. Según la jurisprudencia la organización criminal se caracteriza por una mayor complejidad de su estructura organizativa[81]. Únicamente se hace referencia a la organización criminal, de modo que si se trata de un grupo criminal habrá que apreciar un concurso de delitos con el delito del art. 570 ter.

2. *Daños de especial gravedad o afectado a un número importante de sistemas informáticos*

Partiendo de la misma directiva aludida en el apartado anterior y atendiendo al considerando decimotercero, la Comisión Europea entiende que deben establecerse sanciones más severas cuando «el ciberataque se realiza a gran escala y afecta a un número importante de sistemas de información, en particular cuando el ataque tiene por objeto crear una red infectada o si el ciberataque causa un daño grave, incluido cuando se lleva a cabo a través de una red infectada».

De forma aclaratoria, la Fiscalía en su Circular 3/2017, de 21 de septiembre establece que no es necesario que se den de forma conjunta las dos circunstancias, si no que la agravación es de aplicación cuando se aprecie una u otra.

3. *Daños graves en el funcionamiento de servicios públicos esenciales o afectación a bienes de primera necesidad*

[81] Sobre las organizaciones criminales véase ESCUCHURI AISA, E., «Delitos contra el orden público II», en ROMEO CASABONA/SOLA RECHE/BOLDOVA, *Derecho penal, Parte Especial*, 2.ª ed., Comares, Granada, 2022, pp. 846 y ss.

Dentro del concepto de gravedad no solo se tiene en cuenta el perjuicio económico o patrimonial, sino que también comprende cómo se ha visto afectada la libertad de los propietarios del sistema[82].

En cuanto a lo considerado como «servicios esenciales», concepto amparado por el artículo 128.2 CE, debemos acudir a la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (en adelante, Ley 8/2011) en la cual en el artículo 2 se define como el «servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas»[83]. Además, para identificar los servicios esenciales podemos emplear los criterios esgrimidos en el artículo 6 de la Directiva (UE) 2016/1148: « a) el número de usuarios que confían en los servicios prestados por la entidad de que se trate; b) la dependencia de otros sectores que figuran en el anexo II sobre el servicio prestado por esa entidad; c) la repercusión que podrían tener los incidentes, en términos de grado y duración, en las actividades económicas y sociales o en la seguridad pública; d) la cuota de mercado de la entidad; e) la extensión geográfica con respecto a la zona que podría verse afectada por un incidente; f) la importancia de la entidad para mantener un nivel suficiente del servicio, teniendo en cuenta la disponibilidad de alternativas para la prestación de ese servicio.». En este mismo sentido se pronuncia el TC en su sentencia n.º 26/1981 de 17 de julio (ECLI:ES:TC:1981:26) cuando establece que «la noción de servicio esencial de la comunidad hace referencia a la naturaleza de los intereses a cuya satisfacción la prestación se endereza, entendiendo por tales los derechos fundamentales, las libertades públicas y los bienes constitucionalmente protegidos».

[82] RUEDA MARTÍN, M.ª A., «Los ataques de denegación de servicios como ciberdelito en el Código penal español», *Revista penal* n.º 49, enero 2022, p. 207.

[83] En este sentido, el Anexo II de la Directiva (UE) 2016/1148 sobre los operadores de servicios esenciales, identifica siete sectores de servicios esenciales que han de ser especialmente protegidos frente a los ciberataques. Estos sectores son el energético (electricidad, crudo y gas), transporte, sector sanitario, suministro y distribución de agua potable, banca, infraestructura de los mercados financieros e infraestructura digital. (Directiva 2016/1148/UE, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Diario Oficial de la Unión Europea L194/1 de 19 de julio de 2016). Véase también art. 4 b) Reglamento (UE) 2109/796, del Consejo, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados Miembros.

Así, la razón de esta agravación radica en la importancia que tiene el bien jurídico afectado en esta ocasión. Nos encontramos frente a datos confidenciales que los ciudadanos ofrecen a las Administraciones Públicas en los distintos ámbitos de su vida cotidiana.

En cuanto a los bienes de primera necesidad, estos se definen como aquellos bienes necesarios para la supervivencia ya sean alimentos o productos primarios[84].

4. *Afectación al sistema informático de una infraestructura crítica o creación de una situación de peligro para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea.*

Atendiendo al artículo 2 de la Ley 8/2011, se considera infraestructura crítica a toda infraestructura cuyo funcionamiento es esencial para el mantenimiento de los servicios esenciales del Estado. Asimismo, una infraestructura crítica europea comprende las infraestructuras críticas situadas en algún Estado miembro de la Unión Europea cuya perturbación afectaría a al menos dos Estados; todo ello de acuerdo a la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección. De esta forma, el dañado o borrado de datos tendría un grave impacto al ser infraestructuras no sustituibles. De acuerdo con BARRIO ANDRÉS[85] podríamos concluir que se comprende como sinónimo la creación de una situación de riesgo para el Estado con el ataque a una infraestructura crítica.

Ahora bien, aunque la propia normativa defina las infraestructuras críticas, debemos destacar que tales infraestructuras deben estar recogidas en el Catálogo Nacional de Infraestructuras Estratégicas, elaborado por el Ministerio de Interior.

En el mismo artículo mencionado se establecen los criterios de criticidad y gravedad de las perturbaciones, siendo estos los siguientes: 1º número de personas afectadas, valorado en base al potencial número de víctimas; 2º impacto económico según las pérdidas económicas; 3º impacto medioambiental y por último 4º impacto público y social al dañar la confianza de la población en las Administraciones Públicas.

[84] STS n.º 1307/2006, de 22 de diciembre (ECLI:ES:TS:2006:8332).

[85] BARRIO ANDRÉS, M., *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos,* Wolters Kluver, Madrid, 2018, p. 337.

La razón de esta agravante se encuentra, al igual que en el apartado anterior, en la importancia del objeto material. Estamos frente a sistemas informáticos de infraestructuras críticas que son fundamentales para el correcto funcionamiento de un Estado; es por ello que constituye una ciberamenaza muy relevante, según el Informe de Ciberamenazas y Tendencias Edición 2021 CCN-CERT IA-23/21[86].

Además, en la actualidad encontramos múltiples ejemplos de ataques a infraestructuras críticas. Entre los más recientes, el ataque al Servicio Público de Empleo Estatal (SEPE) a través de un ramsonware que dejo inactiva su web[87] y el ataque al hospital más importante de Asturias a través del que se afectó de forma significativa a la actividad normal de dicha infraestructura crítica[88].

Hay que comentar además, que el artículo 573.1 CP establece que se considerarán como delitos de terrorismo los delitos informáticos tipificados en el artículo 264 CP (entre otros) cuando su finalidad sea alguna de las recogidas en el artículo 573.2 CP, es decir, cuando se pretenda: «1º subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo. 2º Alterar gravemente la paz pública. 3º Desestabilizar gravemente el funcionamiento de una organización internacional. 4º Provocar un estado de terror en la población o en una parte de ella.». En el caso en que concurra alguna de las situaciones descritas, nos situaremos frente a un concurso de normas a resolver por el principio de especialidad de acuerdo al artículo 8.1 CP.

5. Empleo de determinados medios

[86] Véase el Informe de Ciberamenazas y Tendencias Edición 2021 CCN-CERT IA-23/21, elaborado por la Capacidad de Respuesta a Incidentes de Seguridad del Centro Criptológico Nacional (CCN-CERT), p.13

[87] «El SEPE sufre un ataque informático que paraliza sus servicios», disponible en https://www.eleconomista.es/economia/noticias/11093274/03/21/El-SEPE-sufre-un-ataque-informatico-que-paraliza-sus-servicios.html

[88] «Ataque de ransomware contra el hospital más importante de Asturias», disponible en https://www.lavanguardia.com/tecnologia/20211222/7947999/ataque-ransomware-compromete-funcionamiento-hospital-mas-importante-asturias-pmv.html

Estos medios están recogidos en el artículo 264 ter CP y son los siguientes: a) un programa informático, concebido o adaptado principalmente para cometerlo; b) una contraseña de ordenador o código que permita acceder al total o una parte del sistema.

La justificación de esta agravación es la facilitación de la comisión del delito a través de la obtención de una contraseña o código que permita el acceso a los sistemas informáticos mencionados en el artículo 264 CP. Así, lo importante es que la obtención de estos códigos debe realizarse sin autorización del propietario y con la finalidad de cometer el delito. Con todo la Circular 3/2017 insta a una aplicación restrictiva de la agravación limitada a los casos en que se aprecie un plus de injusto.

6. Hechos de extrema gravedad

Para comprender el concepto de extrema gravedad debemos acudir a la Directiva 2014/40/UE la cual expresa que en esta agravante podrían encuadrarse todas aquellas conductas ilícitas que tuvieran consecuencias «apreciables» en los datos, programas o documentos informáticos.

7. Comisión mediante el uso ilícito de datos personales

La agravante recogida en el apartado 3 del artículo 264 CP hace referencia al artículo 9.5 de la Directiva 2014/40/UE por la cual se insta a los Estados a tomar medidas más significativas en aquellas ocasiones en las que la intromisión se haya realizado empleando datos de carácter personal. De acuerdo con RUEDA MARTÍN[89], esta agravante se puede desagregar en tres supuestos:

1. «Aquellos actos en los que el sujeto activo posee los datos sensibles de forma lícita.
2. Actos en los que el sujeto ha obtenido los datos personales de forma ilícita.
3. Situaciones en las que el sujeto se ha encontrado con los datos de forma fortuita sin «haber tomado parte en su descubrimiento».

[89] RUEDA MARTÍN, M.ª A.. «La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico», *cit.*, p. 209.

En cualquiera de estos casos, el sujeto posteriormente comete la infracción tipificada en el artículo 264 CP.

En todo caso se debe tratar de datos personales, es decir, de acuerdo con el Reglamento (UE) sobre Protección de Datos, 679/2016 del Parlamento y del Consejo de 27 de abril y la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se debe tratar de información sobre una «persona identificada o identificable» por ejemplo nombre, apellidos, DNI o número de teléfono, entre otros.

Por otro lado, destacar que la redacción de esta agravante no es igual a la recogida en la Directiva 2013/40/UE pues en esta última se concreta la comisión del delito «utilizando ilícitamente datos de carácter personal de otra persona con la finalidad de ganar la confianza de un tercero, causando así daños al propietario legítimo de la identidad», mientras que en la redacción del CP la aplicación de esta agravante depende de si la utilización ilícita de los datos personales es para facilitarse el acceso al sistema o para ganarse la confianza de un tercero.

En suma, el artículo 264 CP trata de englobar todas las posibles acciones ilícitas capaces de afectar a elementos informáticos abarcando desde la destrucción total o parcial de los mismos hasta su modificación.

Siguiendo con el análisis de los delitos informáticos y en específico de aquellos que persiguen sancionar las conductas que puedan afectar a infraestructuras críticas del Estado, pasamos a estudiar el artículo 264 bis CP.

3. DAÑOS A UN SISTEMA INFORMÁTICO: TIPO BÁSICO DEL ARTÍCULO 264 BIS CP

Con la aprobación de la LO 1/2015, de 30 de marzo, se introdujo el artículo 264 bis en cumplimiento de la Directiva 2013/40 UE[90]. Así, este artículo recoge el tipo básico de

[90] Según el artículo 4 de la citada Directiva: «Los Estados miembros adoptarán las medidas necesarias para que la 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, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad».

obstaculización o denegación de servicios de un sistema informático ajeno de forma grave[91]. Dentro de este artículo estarían comprendidos los ataques DoS y DDos que hemos mencionado anteriormente en los que existe una sobrecarga de un servidor al recibir múltiples solicitudes que impide su funcionamiento correcto.

La inclusión de este precepto con la LO 1/2015, de 30 de marzo resulta fundamental pues la evolución de los ataques DoS y DDoS presenta un fuerte incremento. Atendiendo a las estimaciones llevadas a cabo por organismos nacionales y europeos, resultan la principal amenaza contra el funcionamiento habitual de los sistemas[92].

3.1. Objeto material y acción típica

En este caso, el objeto material no serían los datos y programas informáticos, sino que estaría compuesto por el sistema informático en su conjunto. De acuerdo con la Directiva 2013/40/UE, siguiendo con la definición ofrecida por la Decisión marco 2005/222/JAI del Consejo, los sistemas informáticos comprenden todos los aparatos o grupo de aparatos interrelacionados entre sí, «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». Como indica RODRÍGUEZ MESA, el objeto de la acción es «cualquier sistema informático que se utilice para obtener, almacenar, manipular, administrar, controlar, procesar, transmitir o recibir datos, para satisfacer una necesidad de información[93].

Por otro lado, nos encontramos ante un delito de resultado en el que se enmarcan tres acciones típicas:

- Las acciones recogidas en el artículo 264 CP, ya sean dañar, borrar, deteriorar o hacer inaccesibles los datos o programas informáticos. Cuando la realización de estas conductas además de dañar los datos, programas o documentos, provoca la

[91] VELASCO NÚÑEZ, E./SANCHÍS CRESPO, C., *Delincuencia informática, cit.*, p. 52.

[92] Informe «Internet Organised Crime Threat Assessment 2021» realizado por EUROPOL. También «VIII Informe sobre Cibercriminalidad» realizado por el Ministerio de Interior.

[93] RODRÍGUEZ MESA, M.ª J., *Los delitos de daños, capítulo IX del título XIII del CP tras la reforma de la LO 1/2015, cit.*, p. 91.

obstaculización o interrupción del funcionamiento del sistema, se aplicará solo el art. 264 bis.

- Introduciendo o transmitiendo datos que puedan causar una obstaculización del sistema informático.
- Destruyendo o dañando directamente el conjunto de sistemas informáticos.

Así, las dos primeras acciones corresponden a las recogidas en el artículo 264 CP y en el artículo 5 de la Directiva 2013/40/UE. Ejemplo de estas conductas son los virus «malware» y los ataques de denegación de servicios[94] que ya hemos explicado; estos pueden afectar tanto a datos o programas específicos (encontrándonos en la figura del artículo 264 CP) o a sistemas completos (pasando a calificarse como constitutivos del delito recogido en el artículo 264 bis CP). La tercera de las conductas hace referencia a posibles ataques físicos a los sistemas de almacenamiento o de redes[95]; ejemplo de ello, los cortes de suministro eléctrico o daño a los componentes físicos.

De nuevo, los sistemas informáticos deben ser ajenos. Al igual que en el artículo 264 bis CP, cuando existan dificultades para determinar la propiedad de los sistemas, se interpretará conforme a la existencia o no de habilitación para acceder a los mismos.

Tal y ocurría en el artículo 264 CP, la interrupción de los sistemas informáticos debe ser grave, de tal forma que debe afectar de forma significativa a la normal actividad del sistema informático. Así, nos volvemos a encontrar con trabas interpretativas en tanto en cuanto se trata de un elemento valorativo para el cual no contamos con criterios normativos. De acuerdo con la Circular 3/2017, al hablar de «gravedad» se hace referencia al término «seriously» recogido en la Directiva 2013/40/UE; sin embargo, no ofrece una aclaración en torno a cuándo se considera grave una interferencia, sino que simplemente determina que la actuación debe afectar «realmente y de forma significativa la funcionalidad del sistema atacado, circunstancia que será necesario analizar en cada supuesto en particular».

[94] Véase distintas modalidades de ataques DoS en GIL GIL, A./HERNÁNDEZ BERLINCHES, R. (Coords.), *Cibercriminalidad, cit.*, pp. 221-222.

[95] RODRÍGUEZ MESA, M.ª J., *Los delitos de daños, capítulo IX del título XIII del CP tras la reforma de la LO 1/2015, cit.*, p. 92.

En dicha circular, la FGE indica que hay comportamientos que pueden reconducirse tanto al art. 264 como al art. 264 bis, de manera que habrá que tener en cuenta para aplicar un tipo u otro la capacidad de la acción para afectar a la operatividad o al funcionamiento del sistema en su conjunto. Aquellas acciones que provocan la interrupción u obstaculizan de forma grave el normal funcionamiento de un sistema informático se han considerado por el legislador como más graves y peligrosas.

3.2. Agravantes específicas

En primer lugar, se establece una agravante que plantea su aplicación en el momento en que «los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública», de esta forma, se atiende a las especiales consecuencias que puede tener una interferencia en sectores estratégicos o en la Administración Pública; tal y como expresa la Circular 3/2017 se atenderán a las circunstancias de caso para la aplicación de esta agravante.

Las siguientes agravantes son idénticas a las explicadas en el precepto anterior y por ello, debemos realizar una remisión a los comentarios realizados al respecto en el apartado IV 1º 1.4º de este trabajo. En estos supuestos agravados está prevista la imposición de una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado[96].

También se recoge un tipo agravado (se impone la pena que corresponda en su mitad superior) si los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al programa informático o para ganarse la confianza de un tercero.

Como vemos, a través de esta regulación, el legislador, en concordancia a la Convención de Budapest, trata de dar a los bienes informáticos el mismo tratamiento que a los bienes físicos. Si bien nos encontramos ante dos preceptos similares; a través de su diferenciación, el legislador pretende reflejar la especial gravedad que tiene la interrupción del conjunto de sistemas informáticos.

[96] Critica la previsión de esta pena tan elevada RODRÍGUEZ MESA, M.ª J., *Los delitos de daños, capítulo IX del título XIII del CP tras la reforma de la LO 1/2015, cit.*, p. 94.

4. APROXIMACIÓN A LA APLICACIÓN JURISPRUDENCIAL

Dado que la aplicación del art. 264 o 264 bis depende de la «capacidad de la acción para afectar a la operatividad o al funcionamiento del sistema informático en su conjunto», veremos en este apartado, qué aspectos han considerado los tribunales fundamentales para decantarse por un artículo u otro. Así, vamos a analizar una serie de resoluciones tanto del Tribunal Supremo como de las Audiencias Provinciales.

4.1. Sentencia n.º 737/2016 de la Audiencia Provincial de Barcelona (Sección 7.ª), de 28 de octubre (ECLI:ES:APB:2016:12899)

Esta sentencia hace referencia al caso en el que una extrabajadora efectuó un borrado de datos en el ordenador que tenía asignado en su puesto de trabajo. Entre los datos borrados se encontraba la lista de clientes, muchos de los cuales solo conocía la extrabajadora. Nos encontramos pues dentro del marco del artículo 264 CP. La calificación de la conducta no se discutió, pero en el recurso se analiza si estaba justificada la imposición de la pena de 18 meses de prisión, siendo que el límite mínimo previsto es de 6 meses. Así, este tribunal entiende que este artículo ya incluye de forma connatural cierta gravedad y que, por ello, solo en casos en que concurran otras circunstancias se justificará la aplicación de una pena superior.

4.2. Sentencia n.º 201/2018 de la Audiencia Provincial de Lleida (Sección 1.ª), de 4 de mayo (ECLI:ES:APL:2018:500)

En esta resolución se analiza un supuesto de borrado masivo de correos electrónicos, además de la modificación de la contraseña de dicho correo; lo cual nos sitúa en el artículo 264 CP. Sin embargo, los datos contenidos fueron recuperados gracias a la existencia de una copia de seguridad.

Esta sentencia es especialmente relevante debido a que el tribunal ofrece una extensa argumentación en torno a la necesidad de la existencia de gravedad tanto en la conducta como en el resultado. En primer lugar, entiende que, dado que el artículo 264 CP no ofrece una delimitación de la gravedad de la conducta, esta puede tener distintas modalidades,

desde las más elementales, como podría ser un borrado de datos, hasta las más elaboradas como podría ser el hacking (intrusismo informático) o time bombs («bombas lógicas de acción retardada que destruyen ficheros»). Además, al ser necesaria una gravedad del resultado se deberán tener en cuenta la posibilidad o no de recuperación de los datos borrados, la duración de las tareas de recuperación o incluso la complejidad de las mismas.

Así, en este caso dado que los datos fueron fácilmente recuperables, no se aprecia un delito del artículo 264 CP.

4.3. Sentencia n.º 267/2019 del Juzgado de lo Penal de Madrid (Sección 31.ª), de 4 de septiembre (ECLI:ES:JP:2019:39)

Esta sentencia hace referencia al famoso caso de la destrucción y borrado de datos de los discos duros de los ordenadores de Luis Bárcenas. En este caso, el tribunal entiende que la naturaleza patrimonial del bien jurídico protegido hace que, en aplicación de la doctrina Botín[97], se excluya el ejercicio de la acción penal a las acusaciones populares. Lo relevante de esta sentencia es la acérrima defensa que realiza el tribunal sobre el bien jurídico protegido por el artículo 264 CP. De esta forma establece que en dicho artículo «se tutela penalmente el patrimonio del titular de los elementos informáticos dañados o destruidos».

4.4. Sentencia n.º 220/2020 del Tribunal Supremo, 22 de mayo (ECLI:ES:TS:2020:1520)

Esta resolución va referida a un supuesto en el que una persona elimina 54 carpetas con 1074 archivos informáticos de la empresa con la que mantenía una relación laboral, sin que quede constancia de la existencia de copias de seguridad. Además, el acusado cambió la denominación y los iconos de los archivos borrados para no ser identificados en la «papelera de reciclaje». Con todo, el informático de la empresa consigue recuperar los archivos tres días después.

El Tribunal Supremo considera, en relación con el art. 264 CP, que la gravedad se alcanza cuando «es imposible recuperar la operatividad del sistema»; además, entiende que la

[97] La Doctrina Botín establece que, si el caso solo se mantiene por la acusación popular y, la Fiscalía y la acusación particular desisten, el caso podrá ser sobreseído.

gravedad debe darse tanto en el resultado como en la acción, de tal forma que nos encontramos ante una gravedad «encadenada, acumulativa, que no siempre podrá afirmarse sin dificultad». Como muestra de esta dificultad pone el ejemplo de una acción simple, como el pulsado de teclas y comandos, que genera un grave daño en el sistema; en este caso, y de acuerdo al tribunal, nos encontraríamos un caso dudoso debido a la levedad de la acción y la gravedad del resultado. Concluye que el único momento en que será evidente que el daño funcional es grave será cuando sea imposible recuperar los datos borrados o dañados.

En este caso, y dado que los datos fueron recuperados en tres días, el Tribunal Supremo no estima que nos encontramos ante el ilícito penal recogido en el artículo 264 CP.

Además, un punto fundamental de esta sentencia es la no consideración del delito en grado de tentativa. El Tribunal entiende que el autor hizo todo lo posible por dañar y borrar los datos de forma permanente; así, descarta la argumentación realizada por la sentencia de instancia en la que se defendía que «el acusado realizó todos los actos necesarios para la consumación del delito y, sin embargo, el resultado no se produjo por causas ajenas a su voluntad ya que el sistema operativo guardó los archivos automáticamente en la papelera de reciclaje». El Tribunal Supremo entiende que a través de esta argumentación se elude la gravedad del resultado y que, además, el resultado sí se produjo.

4.5. Sentencia n.º 5/2020 de la Audiencia Provincial de Valladolid, de 8 de junio (ECLI:ES:APVA:2020:440).

En esta ocasión, se analiza un supuesto en el que un individuo, trabajador de un laboratorio, en el año 2017 inhabilitó el funcionamiento de veinte ordenadores utilizando un dispositivo KILLER, un dispositivo capaz de sobrecargar de manera inmediata un ordenador. Tras esta sobrecarga fue necesario reparar todos los ordenadores ocasionando un gasto de 22.130,89€. El Tribunal defiende que la persona es autora de un delito continuado del artículo 264 bis en concurso medial con otro del artículo 264 ter CP al afectar a un sistema informático en su conjunto, habiendo adquirido para ello un instrumento dedicado exclusivamente a la comisión de dicha conducta.

En cuanto a la diferenciación entre el artículo 264 CP y 264 bis, el Tribunal deja claro que el primero de los mencionados debe afectar exclusivamente a «datos informáticos, programas informáticos o documentos electrónicos», mientras que el segundo se refiere a sistemas informáticos en su totalidad. Lo realmente interesante de esta sentencia es el razonamiento ofrecido para contraargumentar la aplicación 264 bis.2 CP en relación al artículo 264.2.2ª CP («Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos»). Entiende que para considerar la acción de «especial gravedad» debería superar el coste económico de 50.000 euros recogido en el artículo 250. 4 y 5 CP («de las defraudaciones») como agravante.

4.6. Sentencia n.º 91/2022 del Tribunal Supremo, de 7 de abril (ECLI:ES:TS:2022:528)

En este caso, una extrabajadora de una empresa decide borrar todos los archivos de un ordenador perteneciente a la empresa, ordenador que empleaba en su actividad laboral. Así, queda constatado que la empresa sufrió graves daños tanto económicos como organizativos. El Tribunal Supremo entiende que, tal y como han apreciado el resto de tribunales, este caso se encuadra en el artículo 264 CP.

Como en la primera sentencia, el Tribunal Supremo defiende que el precepto legal exige un comportamiento grave y, además, una gravedad en el resultado de la acción. Con ello argumenta que la gravedad no debe observarse desde «el mecanismo que se emplee para llevar a término la acción típica», sino que debemos poner nuestro foco de atención en el «daño funcional que el comportamiento genere». Por ello, estima que la gravedad se alcanza cuando «es imposible recuperar la operatividad del sistema o cuando su recomposición es difícilmente reversible». En este caso, el daño es irrecuperable y, además, la empresa tuvo graves problemas funcionales.

VI. CONCLUSIONES

1. Existe una gran preocupación por parte de las autoridades debido al reciente aumento de los delitos informáticos tal y como recoge el informe realizado por INTERPOL para el

año 2020. Cabe destacar, asimismo, que en el marco de la COVID-19 los ataques informáticos aumentaron considerablemente aprovechando la confusión social patente en dicho contexto. Este hecho, sumado a los problemas de interpretación aparejados a los delitos informáticos, hace necesario conocer cómo se articula la respuesta penal a dichas formas de delincuencia.

2. No hay un concepto legal de ciberdelito o de delito informático, tampoco podemos encontrar en nuestro Código Penal un título específico que los regule. Parte de la doctrina entiende que no cabe hablar de «delitos informáticos» ya que el legislador ha optado por diferenciar la comisión de ciertas conductas a través de la vía informática dentro del articulado de castigo de dichas conductas. Sin embargo, la mayor parte de la doctrina considera importante definir las características del «delito informático». En términos generales puede decirse que se ha establecido un concepto muy amplio de ciberdelitos o delitos informáticos, que daría cabida a todos los actos en los que su comisión juegue un papel fundamental un medio informático. Este concepto criminológico incluiría: acciones contra sistemas informáticos; acciones que exigen su comisión por medios informáticos; acciones que se cometen frecuentemente a través de medios informáticos.

En nuestra doctrina ha tenido eco la clasificación propuesta por MIRÓ LLINARES. Este autor clasifica los delitos informáticos en torno a las variables de incidencia de las nuevas tecnologías en la comisión del delito y por el móvil criminológico; encontrando así ciberataques puros (conductas ilícitas que solo pueden ser cometidas a través de las nuevas tecnologías), ciberataques réplica (conductas que ya se daban en la realidad física antes de la introducción de las nuevas tecnologías y que, actualmente, se han adaptado a dichos novedosos medios) y ciberataques de contenido (infracciones cuyo contenido genera el acto ilícito, con respecto a la primera variable y ciberataques económicos, sociales y políticos, con respecto a la segunda.

3. Sin embargo, también encontramos defensores de un concepto más restrictivo en el que tendrían cabida única y exclusivamente aquellos actos ilícitos en los que, bien por el objeto material afectado (el sistema informático), bien por el bien jurídico protegido (la seguridad de los sistemas informáticos), bien por el medio comisivo (los medios informáticos) o bien

por el lugar en el que se producen (el ciberespacio) se genera un aumento de la lesión del bien jurídico y existe dificultad en su persecución.

4. En el ámbito internacional se ha producido una progresiva regulación de los delitos informáticos llegando en la actualidad a contar con un marco normativo internacional, el Convenio de Budapest, a través del cual se establecen una serie de herramientas para hacer frente a la cibercriminalidad global. En el seno de la Unión Europea encontramos múltiples directivas entre las que destaca 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. Además, contamos con la Agencia de Ciberseguridad Europea que se encargar de garantizar la ciberseguridad, ciberresiliencia y confianza dentro de la Unión. En el marco español, si bien no existe una regulación bajo esa denominación en el Código Penal, numerosas son las referencias a delitos considerados como informáticos.

5. Para analizar el impacto de los «delitos informáticos» en nuestro país, hemos empleado las categorías establecidas por el Convenio de Budapest:

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

6. Actualmente también se debate si es posible identificar un nuevo bien jurídico que dote a los delitos informáticos de autonomía propia. Parte de la doctrina jurídica entiende que el bien jurídico protegido por parte de estos delitos está compuesto por la ciberseguridad, es decir, la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos. En base a esta argumentación, dichos autores plantean el traslado de los ciberdelitos en sentido estricto a un nuevo título que agrupe todas las figuras delictivas que vulneran alguno de estos conceptos.

Por el contrario, otro sector de la doctrina jurídica defiende que la aparición de nuevos objetos materiales no justifica la creación de nuevos bienes jurídicos y que, por tanto, nos encontramos ante tipos agravados de otros ya existentes.

7. La regulación de los daños informáticos también ha sido progresiva en nuestro país, ya venían recogidos en el Código Penal desde 1995 si bien con la aprobación de la Ley Orgánica 5/2010, de 22 de junio, en la actualidad se distingue entre daños sobre el sistema informático (art. 264 CP) e interrupciones del funcionamiento del mismo (art. 264 bis CP).

Como muestra del debate anteriormente aludido, con respecto a los arts. 264 y 264 bis parte de la doctrina y también la jurisprudencia defiende –teniendo en cuenta su ubicación sistemática– que el bien jurídico protegido es el patrimonio ajeno, mientras que otros autores consideran que se protege la disponibilidad e integridad de los datos y sistemas informáticos –lo que justificaría su tipificación en un título independiente–.

8. De forma específica, el art. 264 CP tipifica el daño, borrado o deterioro de datos informáticos, programas informáticos o documentos electrónicos ajenos siendo estos su objeto material. Dentro de las conductas típicas encontramos multitud de acciones ya sean más elementales, como un borrado simple, o más elaboradas, como la introducción de malwares o troyanos. De todas formas, es necesario que se produzca gravedad tanto en la conducta como en el resultado. Ambos conceptos, si bien no aparecen delimitados por el Código Penal, son de apreciación en cada caso en particular . Además, el art. 264 CP recoge una serie de agravantes según la acción se cometa en el marco de una organización criminal, se produzcan daños de especial gravedad o afectado a un número importante de sistemas informáticos, los daños graves afecten al funcionamiento de servicios públicos esenciales o a bienes de primera necesidad, la afectación al sistema informático genere una situación de peligro para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea, se empleen medios determinados en el art. 264 ter CP, la conducta sea de especial gravedad o se cometan mediante el uso ilícito de datos personales.

9. En cuanto al artículo 264 bis CP, este comprende la obstaculización o denegación de servicios de un sistema informático ajeno de forma grave, de tal manera que en esta ocasión objeto de la acción es cualquier sistema informático. Dentro de este artículo se recoge una

agravante específica, además de las indicadas para el artículo 264 CP. De esta forma se plantea el tipo agravado cuando los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública.

10. El análisis jurisprudencial realizado pone de manifiesto que para que una conducta pueda ser encuadrada en el artículo 264 o en el 264 bis CP debe reflejar una actuación grave además de un resultado también grave. Ante la indeterminación legal respecto a la gravedad, los tribunales tratan de facilitar criterios, del que destaca en particular atender al «daño funcional que el comportamiento genere».

11. Aun siendo patentes las similitudes entre ambos preceptos, la aplicación de uno u otro dependerá de si la acción afecta a la operatividad o al funcionamiento del sistema en su conjunto o, si se centra en el borrado o deterioro de datos informáticos, programas informáticos o documentos electrónicos ajenos. A través de su diferenciación, el legislador pretende reflejar la especial gravedad e implicaciones que tiene la interrupción del conjunto de sistemas informáticos.

VII. BIBLIOGRAFÍA

ANDRÉS DOMÍNGUEZ, A. C., «Comentarios a los artículos 264, 264 bis, 264 ter y 264 quater», en GÓMEZ TOMILLO, M. (Director), *Comentarios prácticos al Código penal, Tomo III, Delitos contra el Patrimonio y socioeconómicos*, Aranzadi, Pamplona, 2015.

BALEA ROUCO, A., «Copias de seguridad, delito de daños informático y grado de ejecución», *Diario La Ley*, n.º 9939, Sección Doctrina de 25 de octubre de 2021

BARRIO ANDRÉS, M., «La ciberdelincuencia en el Derecho Español*», Revista de las Cortes Generales*, n.º 83, Publicaciones del Congreso de los Diputados, Madrid, 2011.

BARRIO ANDRÉS, M., *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos,* Wolters Kluver, Madrid, 2018.

BORJA JIMÉNEZ, E., *Curso de Política Criminal*, 3.ª ed., Tirant lo Blanch, Valencia, 2021

BUENO ARÚS, F., «El delito informático», *Actualidad Informática Aranzadi,* n.º 11, 1994.

CARRASCO ANDRINO, M.ª del M., «Lección 23ª. Descubrimiento y revelación de secretos» en ÁLVAREZ GARCÍA (Director) y MANJÓN-CABEZA y VENTURA PÜSCHEL (Coords.), *Derecho penal español, Parte Especial (I)*, 2.ª ed., Tirant lo Blanch, 2011.

CEREZO DOMÍNGUEZ, A. I./GARCÍA CORNEJO, R., «La ciberdelincuencia en España: un estudio basado en las estadísticas policiales», *Revista Electrónica de Estudios Penales y de la Seguridad*, 6 (2020). Disponible en www.ejc-reeps.com

CORCOY BIDASOLO, M., «Protección penal del sabotaje informático: especial consideración de los delitos de daños», en MIR PUIG, S. (Coord.), *Delincuencia informática,* Barcelona, 1992.

DAVARA RODRÍGUEZ, M. A., *Manual de Derecho Informático*, Aranzadi, Pamplona, 2015.

DE LA MATA BARRANCO, N., HERNÁNDEZ DÍAZ, L: «El delito de daños informáticos: una tipificación defectuosa» *Estudios Penales y Criminológicos*, vol. XXIX, Servizo de Publicacións da Universidade de Santiago de Compostela, 2009.

DE LA MATA BARRANCO, N., «La tipificación de los denominados "Daños informáticos"», *Revista de Derecho penal*, n.º 26, 2018.

DE LA MATA BARRANCO, N., «Los delitos contra la integridad y disponibilidad de datos y sistemas informáticos después de la LO 1/2015», en BACIGALUPO, FEIJOO, ECHANO (Coords.), *Estudios de Derecho Penal: homenaje al profesor Miguel Bajo,* Ed. Universitaria Ramón Areces, 2016.

DE URBANO CASTRILLO, E., «El acoso y la delincuencia informática», *Revista Aranzadi Doctrinal* núm. 3, 2018.

ESCUCHURI AISA, E., «Delitos contra el orden público II», en ROMEO CASABONA/SOLA RECHE/BOLDOVA (Coords.), *Derecho penal, Parte Especial*, 2.ª ed., Comares, Granada, 2022.

FLORES PRADA, I., *Criminalidad informática*, Tirant lo Blanch, Valencia, 2012.

GALÁN MUÑOZ, A., «*Compliance* frente a delitos informáticos», ABEL SOUTO/BRAGE CENDÁN/GUINARTE CABADA/MARTÍNEZ-BUJÁN PÉREZ/VÁZQUEZ-PORTOMEÑE SEIJAS (Coords.) *Estudios penales en homenaje al Prof. José Manuel Lorenzo Salgado*, Tirant lo Blanch, Valencia, 2021

GIL GIL, A., «Daños informáticos», en SANZ DELGADO, E. y FERNÁNDEZ BERMEJO, D., *Tratado de Delincuencia Cibernética,* Navarra, Aranzadi, 2021.

GIL GIL, A./HERNÁNDEZ BERLINCHES, R., *Cibercriminalidad,* Dykinson, Madrid, 2019.

GONZÁLEZ HURTADO J. A., *Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma,* Tesis doctoral inédita, Madrid, 2013.

GONZÁLEZ RUS, J. J., «Precisiones conceptuales y político-criminales sobre la intervención penal en internet», en *Delito e Informática: algunos aspectos (Cuadernos Penales José María Lidón, n.º 4),* Universidad de Deusto, 2007.

GUTIÉRREZ FRANCÉS, M. L., «Intrusismo informático (hacking). ¿Represión penal autónoma?», *Informática y Derecho,* n.º 12-15, 1994.

HERNÁNDEZ DÍAZ, L. "Aproximación a un concepto de derecho penal informático" en DE LA CUESTA ARZAMENDI (Director)/DE LA MATA BARRANCO, N. (Coord.) *Derecho penal informático,* Civitas, 2010.

LLORIA GARCÍA, P., «Algunas reflexiones sobre el concepto de delito tecnológico y sus características», en GONZÁLEZ CUSSAC J. L. (Director)/LEÓN ALAPONT J. L. (coord.), *Estudios jurídicos en memoria de la profesora doctora Elena Górriz Royo*, Tirant lo Blanch, Valencia.

MATA Y MARTÍN, R. M., «Avances tecnológicos y evaluación de nuevas necesidades iniciales de tutela penal», en ABEL SOUTO/BRAGE CENDÁN/GUINARTE CABADA/MARTÍNEZ-BUJÁN PÉREZ/VÁZQUEZ-PORTOMEÑE SEIJAS (Coords.) *Estudios penales en homenaje al Prof. José Manuel Lorenzo Salgado*, Tirant lo Blanch, Valencia, 2021.

MATA Y MARTÍN, R. M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001.

MESTRE DELGADO, E., «Tema 13. Delitos contra el patrimonio y contra el orden socioeconómico», en LAMARCA PÉREZ (Coord.), *Delitos, La parte especial del Derecho Penal,* Dykinson, Madrid, 2019.

MIRÓ LLINARÉS, F., «Delitos informáticos: Hacking. Daños», en ORTIZ DE URBINA (Coord.), *Memento Experto. Reforma Penal,* Ed. Ediciones Francis Lefebvre, 2010.

MIRÓ LLINARES, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, Madrid, 2012.

MORÓN LERMA, E., *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red,* Aranzadi, 2002.

NAVARRO FRÍAS, I., «Delitos contra el patrimonio y el orden socioeconómico II. Defraudaciones, insolvencias punibles, alteración de precios en concursos y subastas públicas y daños», en ROMEO CASABONA/SOLA RECHE/BOLDOVA PASAMAR

(Coords.), *Derecho penal. Parte Especial conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, Comares, Granada, 2016.

NAVARRO FRÍAS, I., «Delitos contra el patrimonio y el orden socioeconómico II. Defraudaciones, insolvencias punibles, alteración de precios en concurso y subastas públicas y daños», en ROMEO CASABONA/SOLA RECHE/BOLDOVA PASAMAR (Coords.), *Derecho penal. Parte especial*, 2.ª ed., Comares, Granada, 2022.

PICOTTI, L., «Ciberespacio y Derecho penal», en CANCIÓ MELIÁ y otros, *Libro Homenaje al Prof. Dr. Agustín Jorge Barreiro*, UAM, 2019.

PUENTE ABA, L. M., «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿Debe protegerse de forma autónoma la seguridad informática?», en FARALDO CABANA, P (Director)/PUENTE ABA, L. M. (Coord.), *Nuevos retos del derecho penal en la era de la globalización,* Tirant lo Blanch, 2004.

QUINTERO OLIVARES, G., «Art. 264», en Quintero Olivares (Director)/Morales Prats (Coord.), *Comentarios a la Parte Especial del Derecho penal*, 10.ª ed., Aranzadi, Pamplona, 2016.

RODRÍGUEZ MESA, M.ª J., *Los delitos de daños, capítulo IX del título XIII del CP tras la reforma de la LO 1/2015*, Tirant lo blanch, Valencia, 2017.

ROMEO CASABONA, C. M.ª, «De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal», en ROMEO CASABONA (Coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Comares, 2006.

ROMEO CASABONA, C. M.ª, *Poder Informático y Seguridad Jurídica,* Fundesco, 1987.

RUEDA MARTÍN, M.ª A., «La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español»*, Diritto Penale Contemporaneo,* 2020.

RUEDA MARTÍN, M.ª A., «Los ataques de denegación de servicios como ciberdelito en el Código penal español», *Revista penal* n.º 49, enero 2022.

SÁNCHEZ MAGRO, A., «El ciberdelito y sus implicaciones procesales», en GARCÍA MEXÍA P., *Principios de Derecho de Internet*, 2.ª ed., Tirant lo Blanch, Valencia, 2005.

SOLARI MERLO, M., «Análisis de los delitos informáticos. Una propuesta de clasificación», *Revista de Derecho y proceso penal*, n.º 60, 2020.

SOMMER, P y BROWN, I.: OECD «Reducing Systemic Cybersecurity Risk», *OECD project "Future Global Shocks"*, 2011, Accesible en https://www.oecd.org/gov/risk/46889922.pdf

TEJADA DE LA FUENTE, E., «La tipificación penal de los ataques a los sistemas de información», en CAMACHO VIZCAÍNO (Dir.), *Tratado de Derecho penal económico*, Tirant lo Blanch, Valencia, 2019.

TRAPERO BARREALES, P., «Algunas consideraciones en torno al bien jurídico protegido en el delito de daños informáticos», PAREDES CASTAÑON y otros (Dir.) *Libro homenaje al profesor Diego-Manuel Luzón Peña con motivo de su 70º aniversario, vol. II*, Ed. Reus, 2020.

VELASCO NÚÑEZ, E./SANCHÍS CRESPO, C., *Delincuencia informática. Tipos delictivos e investigación con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, Valencia, 2019.

PÁGINAS WEB

Estrategia Nacional de Ciberseguridad 2019. Consultar en https://www.ccn-cert.cni.es/pdf/documentos-publicos/3809-estrategia-nacional-de-ciberseguridad-2019/file.html

Circular 3/2017 de la FGE de 21 de septiembre, sobre la reforma del código penal operada por LO 1/2015, de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos. Consultar en https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2017-00003.pdf

INTERPOL, *Ciberdelincuencia, efectos de la COVID-19,* 2020 accesible en https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

VIII. TEXTOS NORMATIVOS Y CIRCULARES

Circular 3/2017 de la FGE de 21 de septiembre, sobre la reforma del código penal operada por LO 1/2015, de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos.

Código Penal Español.

Constitución Española

Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia

Directiva (UE) 2016/1148 (LCEur 2016, 1042) del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Directiva (UE) 2016/1148 Del Parlamento Europeo Y Del Consejo de 6 de Julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.

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 y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

Reglamento (UE) 2019/796 del Consejo de la Unión Europea, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros

Reglamento (UE) sobre Protección de Datos, 679/2016 del Parlamento y del Consejo de 27 de abril.

IX. JURISPRUDENCIA CITADA

SAP M 480/2017, de 10 de enero (ECLI:ES:APM:2017:480)

SAP SS 708/2019, de 13 de junio (ECLI:ES:APSS:2019:708)

SJP de Madrid 39/2016, de 6 julio (ECLI:ES:JP:2016:39)

STS n.º 1307/2006, de 22 de diciembre (ECLI:ES:TS:2006:8332)

SAP Valladolid n.º 5/2020, 8 de junio de 2020 (ECLI:ES:APVA:2020:440)

STS n.º 220/2020, 22 de Mayo de 2020 (ECLI: ES:TS:2020:1520)

STS n.º 358/2022, de 7 de abril (ECLI:ECLI:ES:TS:2022:528)