Revista Electrónica de Ciencia Penal y Criminología
ISSN 1695-0194

¿Son punibles los daños informáticos imprudentes? Un debate (peligrosamente) abierto*

María A. Trapero Barreales
Universidad de León

TRAPERO BARREALES, MARÍA A. ¿Son punibles los daños informáticos imprudentes? Un debate (peligrosamente) abierto. *Revista Electrónica de Ciencia Penal y Criminología*. 2022, núm. 24-18, pp. 1-34.
http://criminet.ugr.es/recpc/24/recpc24-18.pdf

RESUMEN: El legislador de 1995 ha optado por el sistema de numerus clausus en la incriminación de los delitos imprudentes, pero no ha llevado hasta sus últimas consecuencias esta opción legislativa. La existencia de preceptos penales que actúan como mini cláusulas generales, referidas a los delitos tipificados en un determinado Capítulo, plantean la duda de su verdadero alcance y extensión. Prueba de ello es la controversia doctrinal existente sobre la punibilidad o no de los daños informáticos imprudentes (utilizando la ubicación sistemática para el nomen iuris de estos delitos), alimentada por la forma como se ha estructurado el Capítulo dedicado a los delitos de daños y la redacción dada al art. 267 CP.

PALABRAS CLAVE: daño informático, sabotaje informático, bien jurídico, daño, perjuicio, imprudencia.

TITLE: **Are reckless/negligent computer damages punishable? A (dangerously) open debate**

ABSTRACT: The 1995 legislator has opted for the numerus clausus system in the incrimination of reckless/negligent crimes, but he has not taken this legislative option to its final consequences. The existence of criminal precepts which act as general mini-clauses, referring to crimes defined in a certain Chapter, raise the doubt of their true scope and extension. Evidence of this is the existing doctrinal controversy over the punishability or not of reckless/negligent computer damages (using the systematic location for the nomen iuris of these crimes), fueled by the way in which the Chapter dedicated to crimes of damages has been structured and the wording given to the article 267 of the Spanish Penal Code.

KEYWORDS: computer damage, computer sabotage, legal protected interest, damage, harm, recklessness/negligence.

Fecha de recepción: 15 enero 2022

Fecha de publicación en RECPC: 30 mayo 2022

Contacto: matrab@unileon.es

SUMARIO: I. Introducción. II. A favor de la punibilidad de los daños informáticos imprudentes. 1. Antes de las reformas de 2010 y 2015. 2. Después de las reformas de 2010 y 2015. 3. Argumentos a favor de la punibilidad de los daños informáticos imprudentes. III. En contra de la punibilidad de los daños informáticos imprudentes. 1. La opinión doctrinal. 2. Otros argumentos en contra de la punibilidad de los daños informáticos imprudentes. IV. Recapitulación. Bibliografía.

---

* Este trabajo se enmarca en el Proyecto de investigación PID2019-108567RB-C21 (AEI), así como en las tareas de investigación de la UIC 166 de Castilla y León; en ambos casos el investigador principal y director es el Prof. Dr. Dres. h. c. Miguel Díaz y García Conlledo y en el PID2019 es segunda IP la Prof. Dra. María A. Trapero Barreales.

I. **Introducción**

Tomando en consideración los principios limitadores de la potestad punitiva del Estado, principalmente, pero no solo, los de intervención mínima, carácter fragmentario y *ultima ratio*, en el vigente CP se ha optado por el sistema de *numerus clausus-crimina culposa* en la tipificación de los delitos imprudentes[1].

Así se establece sin ningún género de dudas en el art. 12 CP: "Las acciones u omisiones imprudentes sólo se castigarán cuando *expresamente* lo disponga la ley".

Con este precepto como brújula, en el Libro II del CP se ha hecho la selección correspondiente de los delitos imprudentes, como regla general, limitando la tipificación penal a que el hecho se cometa con imprudencia grave (por ejemplo, arts. 146, 324, 332.3, 334.3 CP), de manera excepcional previendo la intervención penal ante la comisión del hecho con imprudencia grave o menos grave (en los arts. 142 y 152 CP).

Pero la opción por el sistema de *numerus clausus* no ha desterrado completamente el recurso a algunas técnicas legislativas, eso sí, ahora a pequeña escala, que recuerdan a la antigua incriminación de la imprudencia a través de cláusulas generales; el recurso a este tipo de técnicas regulatorias genera la duda sobre el verdadero alcance y extensión de la incriminación de la imprudencia.

Porque a veces se ha optado por un precepto penal que incrimina el/los delitos imprudentes que están tipificados en un determinado Capítulo. Por ejemplo, esto sucede en el Título XVII del Libro II, en el Capítulo II, de los incendios, en concreto en el art. 358 CP, donde se prevé la tipificación de los delitos de incendio descritos en los arts. 351 a 357 CP cometidos por imprudencia grave. O en el Título XVI del Libro II, en el Capítulo III, de los delitos contra los recursos naturales y el medio ambiente, en el art. 331 CP, donde se prevé la tipificación de los hechos previstos en este Capítulo cuando se cometan con imprudencia grave.

Otras veces se ha optado por un precepto que incrimina el/los delitos imprudentes

[1] Para más detalles, por todos, LUZÓN PEÑA, 2016, pp. 300 y ss.

tras la enumeración de una serie más o menos extensa de delitos dolosos. Esto sucede, por ejemplo, dentro del Título XVII del Libro II, en el Capítulo III: tras la tipificación de los delitos contra la salud pública dolosos en los arts. 359 a 366 CP aparece el art. 367 CP, precepto en el que se tipifican los delitos contra la salud pública descritos anteriormente cometidos con imprudencia grave. O en el Capítulo I, sección 1ª: tras la tipificación de los delitos relativos a la energía nuclear y a las radiaciones ionizantes dolosos en los arts. 341 a 343 aparece el art. 344 CP, precepto en el que se tipifican los hechos descritos anteriormente cometidos con imprudencia grave.

Y otras veces, en lo que aquí interesa, se ha recurrido a un precepto que cierra la tipificación de determinados delitos ubicados en un Capítulo, donde aparecen descritas varias figuras delictivas dolosas y el último precepto, redactado de manera genérica, prevé la comisión imprudente (cuando la imprudencia sea grave). Esto es lo que sucede en el Título XIII del Libro II CP, dedicado a los delitos contra el patrimonio y el orden socioeconómico, en el Capítulo IX relativo a los daños: en los arts. 263 a 266 CP se enumeran una serie de delitos de daños dolosos, entre ellos aparecen tipificados, en los arts. 264 a 264 quater CP, los delitos de daños informáticos (utilizando la rúbrica del Capítulo para su denominación)[2], y en el art. 267 CP, cerrando el Capítulo IX, se castigan los daños causados con imprudencia grave (si superan la cuantía de 80.000 euros).

La forma como se ha estructurado este Capítulo IX abre el interrogante sobre la punibilidad o no de los daños informáticos imprudentes.

La cuestión que aquí nos va a ocupar no ha sido objeto de especial explicación por la doctrina[3]; el interés se ha centrado en otros aspectos que resultan problemáticos en la interpretación de los delitos de daños informáticos dolosos. En particular, en el

[2] No hay unanimidad en el *nomen iuris* de los delitos tipificados en los arts. 264 a 264 quater. Son varias las expresiones utilizadas para su denominación: entre otras, vandalismo informático, cracking, cyberpunking, o las más habituales, daños informáticos, sabotaje informático. O, desde la regulación actual, se utilizan dos denominaciones, daños informáticos para los hechos del art. 264 y sabotaje informático para los hechos del art. 264 bis. Recurren al término daños informáticos, entre otros muchos, DE LA MATA/HERNÁNDEZ, 2009, pp. 311, 315 s.; 2010a, pp. 161y ss.; 2010b, 204 y ss. Utilizan el *nomen iuris* sabotaje informático, entre otros, ANDRÉS DOMÍNGUEZ, 1999a, p. 1724; 1999b, pp. 111, 142 s.; ROBLES/PASTOR, 2021, p. 304, quienes diferencian entre sabotaje a datos y sabotaje a sistemas informáticos; siguiéndoles, GORJÓN BARRANCO, 2021, p. 81 n. 10.

[3] De momento, salvo error por mi parte, este debate no se ha planteado jurisprudencialmente. Pero quizás se puede aventurar que la respuesta sería favorable a la punibilidad de los daños informáticos imprudentes. A esta deducción se puede llegar desde el momento en que la excusa absolutoria regulada en el art. 268 CP sí se ha aplicado judicialmente a los delitos de daños informáticos. Esto ha sucedido en el AAP M 28 de febrero 2019 (ECLI:ES:APM:2019:880A). Y es que la regulación de la excusa absolutoria prevista en este precepto sigue el modelo de la regulación de los daños imprudentes del art. 267: aquí se refiere genéricamente a los daños causados por imprudencia grave, allí a la exención de responsabilidad criminal por los delitos patrimoniales que se causaren entre sí determinados parientes. El argumento utilizado en el Auto acabado de citar es que en el delito de daños informáticos el bien jurídico protegido sigue siendo el patrimonio por lo que resulta aplicable, por su ubicación sistemática, la norma contenida en el art. 268 CP.

art. 264.1, cómo se ha de valorar el requisito referido a la gravedad exigido doblemente, respecto de la acción típica relacionada con el objeto material y del resultado derivado de ella, o en el art. 264 bis.1, la gravedad referida a la obstaculización o interrupción del funcionamiento del sistema informático; los parámetros que han de ser tomados en consideración para dar contenido al resultado daño (y verbos semejantes) grave/obstaculización-interrupción grave; en relación con esta cuestión, si se ha de exigir o no la superación de una determinada cuantía económica para la aplicación de los arts. 264.1/264 bis.1; cómo afecta a la interpretación de estos delitos el hecho de que el sujeto pasivo cuente con copias de seguridad; cómo se han de interpretar las circunstancias cualificantes previstas en los arts. 264.2-3 y 264 bis.1 segundo párrafo-2 y 3; y, sobre todo y principalmente, porque repercute en todos los anteriores, el aspecto más debatido es el relativo al bien jurídico protegido en los delitos de daños informáticos, pues conecta con la discusión genérica sobre la aparición o no de nuevo/s bien/es jurídico/s protegible/s a través de (algunos de) los delitos informáticos o, como nueva generación, los ciberdelitos, y, como cuestión previa, el mismo concepto de delitos informáticos y de ciberdelitos[4].

Volviendo al tema que nos ocupa, si son o no punibles los daños informáticos imprudentes a través del art. 267 CP, es preciso advertir que la respuesta ofrecida doctrinalmente se ha podido ver influida por la propia regulación de los daños informáticos dolosos, muy diferente en su versión originaria, en el antiguo art. 264.2, a la que hoy está en vigor, con una primera y sustancial modificación en la reforma aprobada por la LO 5/2010, de 22 de junio, mejorada y ampliada mediante la LO 1/2015, de 30 de marzo. Por esta razón, en la exposición sobre el estado de la opinión doctrinal sobre la punibilidad de los daños informáticos imprudentes se hará referencia a las opiniones defendidas antes y después de las reformas de 2010-2015, de manera específica en la exposición de la tesis que contesta afirmativamente a dicha cuestión.

[4] Desde hace tiempo se debate vivamente sobre los conceptos, primero de delitos informáticos (o expresiones similares), posteriormente de ciberdelitos (o expresiones parecidas), por un lado, y, derivada de esta conceptualización, por otro lado, de las clasificaciones de los delitos informáticos, en un primer momento, actualmente de los ciberdelitos. El debate, conceptual y clasificatorio, viene influenciado por el relativo a si estos avances técnicos han supuesto la aparición de nuevos objetos de protección y/o nuevos objetos materiales-nuevas formas de ataque a "viejos" bienes jurídicos. Sobre todas estas cuestiones, v., por todos, MATA Y MARTÍN, 2001, *passim*; 2021, pp. 895 y ss.; CRUZ DE PABLO, 2006, pp. 20 y ss.; PICOTTI, 2006, pp. 329 y ss.; ROMEO CASABONA, 2006, pp. 5 y ss.; 2007, pp. 653 y ss.; CORCOY BIDASOLO, 2007, pp. 9 y ss.; DE LA MATA BARRANCO, 2007, pp. 43 y ss.; FERNÁNDEZ TERUELO, 2007, *passim*; GONZÁLEZ RUS, 2007, pp. 13-38; MAZUELOS COELLO, 2007, pp. 43 s.; HERNÁNDEZ DÍAZ, 2009, pp. 230 y ss.; 2010, pp. 36 y ss.; DE URBANO CASTRILLO, 2012, pp. 19 s., 29; MIRÓ LLINARES, 2012, pp. 33-139; BARRIO ANDRÉS, 2016, pp. 2 y ss., 9 y ss.; 2018, pp. 31 y ss., 65-184; DAVARA/DAVARA/DAVARA (coord.), 2017, pp. 25-186, 207-233; ALMENAR PINEDA, 2018, *passim*; LIRA ARTEAGA, 2018, pp. 27-119; CÁMARA/CANO/GARCÍA/GIL (coord.)/HERNÁNDEZ (coord.)/MARTÍN/PASTOR/ROBLES/TOBARRA, 2019, pp. 141-286; VELASCO NÚÑEZ, 2019, pp. 21-251; VIDAURRI ARÉCHIGA, 2019, pp. 204 y ss.; LÓPEZ MUÑOZ, 2020, pp. 23 y ss.; MESTRE DELGADO, 2021b, pp. 48 ss., 58 ss.

II. **A favor de la punibilidad de los daños informáticos imprudentes**

1. ***Antes de las reformas de 2010 y 2015***

En este momento el delito de daños informático tenía otra estructura y otra descripción típica: estaba previsto en el antiguo art. 264.2; en el antiguo art. 264.1, conminado con la misma pena, se describían y enumeraban las circunstancias cualificantes que hoy aparecen mencionadas en el art. 263.2 CP.

Esta estructura del antiguo precepto, y su ubicación sistemática, había generado una viva discusión doctrinal sobre su naturaleza; en esta polémica contribuyó el diferente tenor literal de los apartados 1 y 2 del antiguo art. 264[5]. Para un sector de la doctrina el delito de daños informático era un tipo agravado o cualificado del delito de daños[6], mientras que otro sector doctrinal ya en este momento ha reconocido que era un delito autónomo o especial, discutiéndose si se limitaba a los daños en el objeto material identificado con los datos, programas y documentos electrónicos o también se subsumía en él los daños en los elementos físicos donde estaban ubicados tales objetos materiales[7].

La discusión sobre su naturaleza tenía repercusión sobre su interpretación. Reconociendo que era un delito especial o autónomo, en ocasiones la exégesis se ha fijado tomando en consideración que se trataba de un delito de daños, porque así se deducía también de su ubicación sistemática, con repercusión todo ello en el bien jurídico protegido por aquella figura delictiva[8], mientras que en otras ocasiones se ha defendido que se estaba en presencia de un delito autónomo porque así se tenía que deducir

[5] Ampliamente sobre la discusión doctrinal en torno a la naturaleza del antiguo delito de daños informático, GONZÁLEZ RUS, 2002, pp. 1288 y ss.; 2005a, pp. 785 y ss.; 2006, pp. y 253 s.

[6] V., de esta opinión, MARCHENA GÓMEZ, 2001, pp. 358, 363; MATA Y MARTÍN, 2001, p. 80; GARCÍA ARÁN, 2004, pp. 930 s.; GARCÍA GONZÁLEZ, 2005, pp. 772, 776, si bien reconoce que hay razones para la creación de un tipo autónomo; CRUZ DE PABLO, 2006, p. 37; FERNÁNDEZ TERUELO, 2007, pp. 112 s.; RODRÍGUEZ MESA, 2017, pp. 53 s.

[7] A favor de la tesis de que era un delito autónomo referido solo a los daños en los elementos lógicos, por tanto, si la misma conducta causa daños en elementos lógicos y en elementos físicos hay que aplicar el concurso ideal de delitos entre los arts. 263 y 264.2, por todos, ANDRÉS DOMÍNGUEZ, 1999a, p. 1727; 2009, pp. 416 s. A favor de la tesis de que era un delito autónomo que abarcaba los daños en elementos físicos y lógicos, por todos, GONZÁLEZ RUS, 2002, pp. 1295 s.; 2005a, pp. 785 s.; 2005b, p. 1471.

[8] A favor de la interpretación del antiguo delito de daños informático como tipo autónomo o especial, pero en todo caso se protegía la propiedad, pues así se derivaba además de su ubicación sistemática en el título dedicado a delitos contra el patrimonio y el orden socioeconómico, y su interpretación había de hacerse siguiendo la teoría general del delito de daños (sea cual sea la forma como se entienda esta teoría general en cada caso), a veces exigiendo superar la cuantía económica fijada en el tipo básico de daños, otras veces este no era un requisito típico, entre otros, GONZÁLEZ RUS, 1999, p. 4; 2002, pp. 1295 y ss.; 2005a, pp. 785, 789 s., 791; 2005b, pp. 1470 s., 1476, 1477; 2006, pp. 253 s., 258, 259; 2007, pp. 13 s., 28, 29 y ss., 34, 36 s., descartando aquí las formulaciones teóricas sobre la aparición de nuevos bienes jurídicos necesitados de protección penal como consecuencia del desarrollo de la informática y las Tic`s (solo admite la aparición de un nuevo bien jurídico, el derecho a la autodeterminación informativa); ORTS/ROIG, 2001, pp. 79, 81; CORCOY BIDASOLO, 2007, pp. 18, 30; MARCHENA GÓMEZ, 2001, p. 358. Por su parte, FERNÁNDEZ/MORALES, 2000, p. 1524, planteaban la doble lectura del antiguo art. 264.2, como tipo cualificado de daños, como tipo autónomo, en ambos casos se tenía que valorar el daño desde una perspectiva funcional.

desde el momento en que en él se protegía un nuevo bien jurídico surgido del avance y desarrollo de la informática y/o de las técnicas de información y comunicación (TIC`s), y/o se protegía un bien jurídico que no era estrictamente el patrimonio, aun cuando su ubicación sistemática hiciera pensar otra cosa[9].

Desde una u otra tesis doctrinal sobre la naturaleza (tipo autónomo/tipo cualificado) y el bien jurídico tutelado por el antiguo delito de daños informáticos (patrimonio/un nuevo bien jurídico) se ha admitido expresamente la punibilidad de los daños informáticos imprudentes a través del art. 267 CP, cumpliéndose, claro está, los requisitos que este precepto exigía (y exige) para la comisión imprudente[10].

El reconocimiento de que el objeto de protección en el delito de daños informático

[9] Ya en esta primera etapa para un amplio sector de la doctrina, el desarrollo, primero de la informática, posteriormente de las TIC`s, ha supuesto la aparición de nuevo/s bien/es jurídico/s, de carácter supraindividual generalmente (si se reconoce que han aparecido varios bienes jurídicos, algunos serán de carácter individual, otros serán supraindividuales). Véase, entre otros muchos, ÁLVAREZ VIZCAYA, 2001, pp. 274 y ss.; 278; QUINTERO OLIVARES, 2001, p. 371; CORCOY BIDASOLO, 2007, p. 10; MORALES PRATS, 2007, pp. 227, 230; y ampliamente HERNÁNDEZ DÍAZ, 2009, pp 230 y ss., 236 y ss.; 2010, pp. 36 y ss., 45 ss. En el caso de los daños informáticos, este bien jurídico es la accesibilidad e integridad de la información y de los sistemas informáticos para RODRÍGUEZ/ALONSO/LASCURAÍN, 2001, p. 285; o la disponibilidad e integridad de datos y sistemas informáticos para DE LA MATA BARRANCO, 2007, pp. 49 s.; DE LA MATA/HERNÁNDEZ, 2009, pp. 324, 329 s., 331 s., 332, 333, 348; 2010a, pp. 161; 2010b, pp. 212 s., 217, 218 s., 220 s., 236; 2011, pp. 643, 648, 649, 650 s., si bien reconociendo que, por su ubicación sistemática, se trata de un delito contra el patrimonio; o la seguridad de las redes y los sistemas informáticos para CARRASCO ANDRINO, 2009, p. 344, para garantizar la disponibilidad, autenticidad e integridad de los datos y de los servicios que ofrecen dichas redes o sistemas; HERNÁNDEZ DÍAZ, 2009, p. 241; 2010, p. 52. A esta conclusión sobre la aparición de un nuevo bien jurídico a proteger en el delito de daños informático también parece que llega ANDRÉS DOMÍNGUEZ, 1999a, pp. 1726 s.; 1999b, p. 143; 2009, pp. 416 s., 419, 422, 423. La necesidad de protección de nuevos bienes jurídicos ya se había planteado durante la vigencia del antiguo CP, cuando aún no se habían tipificado expresamente los daños informáticos. V., en este sentido, por todos, CORCOY BIDASOLO, 1990, p. 1016 (=1992, pp. 175 s.). En la interpretación del delito de daños informáticos se ha afirmado que se protegen intereses económicos que no se pueden identificar con el patrimonio en sentido estricto, entre otros, por GUTIÉRREZ FRANCÉS, 1996, pp. 252 s., 274, 291, 297, si bien hay que advertir que en este comentario se está centrando en la explicación del sabotaje informático que afecta a la actividad empresarial; MATELLANES RODRÍGUEZ, 2000, pp. 132 s., 138 s., 141, 142, relacionando estos intereses económicos con la capacidad competitiva de la empresa; MORÓN LERMA, 2002, p. 67; 2007, pp. 118 n. 81, 123, 125, 126, aquí ya haciendo alusión a las directrices de la UE a favor de la aparición de un nuevo bien jurídico, el correcto funcionamiento de los sistemas informáticos, concluyendo que nos encontramos ante un ámbito de criminalidad necesitado de autonomía, y el reconocimiento del nuevo valor o bien jurídico resulta casi *indiscutible* (cursiva destacada por mí); 2010, pp. 246 s.

[10] Así, sea un delito agravado, sea un delito autónomo, referido solo a los elementos lógicos o que abarca tanto elementos lógicos como físicos, pero en todo caso conectando la tipificación de los daños informáticos con el bien jurídico propiedad, han admitido expresamente la punibilidad de los daños informáticos imprudentes, MATA Y MARTÍN, 2001, p. 76; ORTS/ROIG, 2001, p. 84, si bien advierten que el art. 267 está pensado para los daños materiales; GONZÁLEZ RUS, 2002, p. 1298; 2005a, pp. 790, 797; 2005b, pp. 1476, 1484; 2006, pp. 258, 269; FERNÁNDEZ TERUELO, 2007, p. 121. Desde la tesis de que nos encontramos ante un delito económico (se protege algo más o algo diferente al patrimonio), admiten la punibilidad de los daños informáticos imprudentes, GUTIÉRREZ FRANCÉS, 1996, p. 299; MORÓN LERMA, 2002, pp. 67 s. Desde la tesis de que se protege el bien jurídico integridad y disponibilidad de datos, programas y documentos electrónicos, admiten la punibilidad de los daños informáticos imprudentes, ANDRÉS DOMÍNGUEZ, 1999a, p. 1727; 2009, p. 422 (aunque esta autora no ha afirmado expresamente que este sea el bien jurídico protegido en los daños informáticos); RODRÍGUEZ/ALONSO/LASCURÁIN, 2001, p. 285; DE LA MATA BARRANCO, 2007, pp. 49 s., 50; DE LA MATA/HERNÁNDEZ, 2009, pp. 350, 351; 2010a, pp. 161, 163; 2010b, pp. 237, 239.

no es en realidad el patrimonio, o más específicamente, la propiedad, no ha sido un impedimento para apoyar esta conclusión. Parece que su ubicación sistemática en el Capítulo dedicado a los delitos de daños, y la forma como se ha estructurado el mismo, han sido argumentos de peso para apoyar aquella interpretación.

2. *Después de las reformas de 2010 y 2015*

A partir de la reforma de 2010, y posteriormente la de 2015, la doctrina de manera unánime ha reconocido que los daños informáticos son delitos autónomos o especiales[11]. La nueva estructura de los delitos de daños ha servido para aclarar esta circunstancia: a partir de 2010 en el art. 263 CP aparecen tipificados el delito básico y los tipos cualificados de daños; el art. 264 CP se reserva para los daños informáticos, y esta estructura se mantiene en 2015, ocupando los daños informáticos los arts. 264 a 264 quater CP.

Si la regulación de los daños informáticos ha cambiado de manera sustancial, como consecuencia primero de la transposición de la Decisión Marco 2005/222/JAI, del Consejo, de 24 de febrero, y después de la Directiva 2013/40/UE, del Parlamento y del Consejo, de 12 de agosto, sin embargo su ubicación sistemática se ha mantenido inalterada, circunstancia que ha sido objeto de crítica por un amplio sector doctrinal[12]. Esta regulación legal ha afectado a la forma como se ha explicado el bien jurídico protegido a través de estas figuras delictivas (algo que ya sucediera en la versión originaria de los daños informáticos, como se ha explicado en el apartado anterior), pues esto ha llevado a mantener que el objeto de protección ha de conectarse con esta ubicación entre los delitos contra el patrimonio y el orden socioeconómico, en el capítulo relativo a los delitos de daños[13]. Para otro sector doctrinal, siguiendo el planteamiento ya propuesto antes de las reformas de 2010 y 2015, los delitos de daños

[11] Así lo afirman expresamente, entre otros muchos, FERNÁNDEZ TERUELO, 2010, p. 251; 2011, pp. 96, 100; MIRÓ LLINARES, 2010, nm. 1477, 1479/(p. 157); RAGUÉS/ROBLES, 2012, p. 373; ROMEO CASABONA, 2012, pp. 367, 370 (=2013, pp. 650, 653); CORCOY BIDASOLO, 2015, p. 932; 2019, p. 579; RODRÍGUEZ MESA, 2017, pp. 57 s.; LÓPEZ MUÑOZ, 2020, p. 72.

[12] A favor de la reubicación, sea en un título, capítulo o sección, donde estarían este y otros delitos informáticos o ciberdelitos, entre otros muchos, ANDRÉS DOMÍNGUEZ, 1999a, p. 1727; 1999b, pp. 109, 143; 2009, p. 423; 2011, p. 436; 2015a, p. 549; MORALES PRATS, 2007, p. 230; MORÓN LERMA, 2007, pp. 125 s.; 2010, p. 246; DE URBANO CASTRILLO, 2007, p. 2125; 2012, p. 29; CARRASCO ANDRINO, 2009, pp. 355 s.; DE LA MATA/HERNÁNDEZ, 2009, pp. 331, 349; 2010b, pp. 218 s., 237; 2011, p. 650; DE LA MATA BARRANCO, 2010, pp. 153, 156, 159; 2016a, pp. 1093, 1096; 2016b, pp. 55 s., 83 s.; 2018, pp. 742, 744; ROMEO CASABONA, 2012, p. 369 n. 75 (=2013, pp. 651 s. n. 75); GONZÁLEZ HURTADO, 2014, pp. 4 s.; 2016, pp. 68 s.; RODRÍGUEZ MESA, 2017, p. 66; BARRIO ANDRÉS, 2018, p. 107; CÁMARA/CANO/GARCÍA/GIL (coord.)/HERNÁNDEZ (coord.)/MARTÍN/PASTOR/ROBLES/TOBARRA, 2019, p. 150; GIL GIL, 2021, pp. 468, 470; GORJÓN BARRANCO, 2021, pp. 99 s., 110; PÉREZ BES (coord.), 2021, nm. 2870/(p. 279).

[13] Esta parece ser la tesis de FERNÁNDEZ TERUELO, 2010, pp. 250, 251; 2011, p. 96. También toman en consideración esta ubicación sistemática, CORCOY BIDASOLO, 2015, p. 934; 2019, p. 581; ESTRADA CUADRAS, 2016, nm. 4629, 4635, 4703, 4717, 4730/(pp. 520 s., 521, 529, 531), recurriendo también al argumento de la conminación de algunas modalidades delictivas con la pena de multa proporcional; RÍOS CORBACHO, 2016, p. 441; ECIJA, 2019, nm. 8206/(p. 715); NIETO MARTÍN, 2019, pp. 215, 217, 219, aceptando que la seguridad informática inspira parte de las circunstancias cualificantes previstas en los arts. 264.2 y 264 bis.2. Este autor sí reconoce que en el art. 264 ter, un tipo penal que castiga actos preparatorios

informáticos pertenecen a los delitos informáticos y, en la actualidad, a los ciberdelitos puros o en sentido estricto, que han de proteger nuevo/s bien/es jurídico/s surgido/s con el desarrollo de la informática y posteriormente de las TIC,s[14], sea este identificado genéricamente como la seguridad informática o seguridad en los sistemas de información[15], o el correcto funcionamiento de redes y sistemas informáticos[16], sea planteado de manera específica en los daños informáticos como la integridad y disponibilidad de datos y redes y sistemas informáticos[17].

de los daños informáticos, solo se entiende si se conecta con el bien jurídico colectivo seguridad de los sistemas de información (pp. 219 s.); BENÍTEZ ORTÚZAR, 2020, pp. 662, 667 s., señalando que, en su contenido, el art. 264 está más cerca de la indemnidad de los datos o de la propia seguridad informática; GUTIÉRREZ (coord.)/CASTRO/PÉREZ, 2021, p. 53; ZUGALDÍA ESPINAR, 2021, p. 313. Por su parte, MIRÓ LLINARES, 2010, nm. 1482, 1485, 1510/(pp. 158, 159, 165), en su comentario a la forma como ha transpuesto el legislador español la Decisión Marco 2005/222/JAI, afirma que no se puede negar la relación del delito de daños informático con el patrimonio. También FERNÁNDEZ DÍAZ, 2018, pp. 2, 3, 10 s., 14 s., 22 s., parece admitir que se protege el patrimonio, entendido desde un concepto funcional; en concreto, en los daños informáticos se protegería la información como elemento de valor económico que es parte de la propiedad de la empresa y que ha de ser protegida frente a ataques a su integridad y disponibilidad (la confidencialidad sería objeto de protección a través de otras figuras delictivas). Con mayor claridad, MESTRE DELGADO, 2021b, pp. 52, 54, 56., descarta que en los delitos de daños informáticos se esté protegiendo un nuevo bien jurídico, es el patrimonio el objeto de protección. Estos delitos los incluye en la clasificación referida a la infraestructura informática, electrónica o cibernética como objeto de la agresión, parte integrante del patrimonio de las personas, físicas o jurídicas (p. 60).

[14] Si se admite que existen diferentes delitos informáticos o, como categoría diferente, evolucionada, ciberdelitos, por un lado, los que protegen de manera principal bienes jurídicos "tradicionales", por otro lado, los que podrían calificarse como ciberdelitos puros, será sobre todo en relación con estos últimos donde se plantea de manera más evidente la posible aparición de un nuevo bien jurídico. Y a este grupo de ciberdelitos puros pertenecerían los delitos de daños informáticos y/ o sabotaje informático.

[15] Afirman de manera indubitada que los daños informáticos han de proteger un nuevo bien jurídico, la seguridad informática, ANDRÉS DOMÍNGUEZ, 2011, p. 436; RODRÍGUEZ MESA, 2017, pp. 64 ss., bien jurídico macrosocial que se concreta en la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos; estos dos últimos elementos son los que se garantizan a través de los delitos de daños informáticos. Esta autora aclara que se está ante un bien jurídico autónomo que no es identificable, ni con el patrimonio, ni con la intimidad; GIL GIL, 2021, pp. 468 s., añadiendo que, a la vista de la ubicación sistemática de los daños informáticos, el legislador ha optado por centrarse en el bien jurídico al que mediatamente sirve la ciberseguridad, el patrimonio y el orden socioeconómico, pero concluye esta autora que, a pesar de esta ubicación, los daños informáticos protegen un bien jurídico colectivo que va más allá del patrimonio (p. 470); GORJÓN BARRANCO, 2021, pp. 99 s., 110, 120, si bien por la ubicación sistemática este bien jurídico se debe interpretar en clave patrimonial, desde la tesis funcional. Esta autora añade que en las circunstancias cualificantes se percibe con más claridad el nuevo bien jurídico. A favor de la concreción del nuevo bien jurídico aparecido con el desarrollo de la informática y de las TIC,s como seguridad en los sistemas de información, GONZÁLEZ HURTADO, 2014, pp. 2 s., 3 ss., 5 s.; 2016, pp. 60 ss., 62 ss., 68 ss., 70 ss., 74, un bien jurídico colectivo que ha de protegerse tipificando delitos de lesión y delitos de peligro. Reconoce este autor que en el CP no se ha consagrado este nuevo bien jurídico. Y concluye afirmando que los daños informáticos protegen el patrimonio (pp. 3, 5; 65, 71).

[16] LÓPEZ MUÑOZ, 2020, p. 23.

[17] V., en este sentido, DE LA MATA BARRANCO, 2010, pp. 155, 158 ss.; 2016a, pp. 1092 s., 1095, 1097 s., 1098; 2016b, pp. 57, 76 s.; 83 s.; 2018, pp. 743, 744; SALVADORI, 2011, pp. 224, 227, 241; PÉREZ BES (coord.), 2021, nm. 2870/(p. 279), criticando la ubicación sistemática seguida por el legislador español, al incluir estos delitos como tipos especiales en el capítulo dedicado a los daños. Esta ubicación lleva a entender, incorrectamente, que se protege el patrimonio o la propiedad (nm. 2767/p. 263). Plantea como bien jurídico colectivo (con una función negativa y otra positiva) la confidencialidad, la integridad y la disponibilidad de los sistemas de información, protegido en el art. 264 bis (y en los arts. 197 bis y 197 ter), RUEDA MARTÍN, 2021, pp. 1312-1320, aclarando que, en su dimensión o función negativa, este bien jurídico colectivo constituye una barrera de contención de riesgos para otros bienes jurídicos, entre otros, la intimidad personal y

Sea cual sea el objeto de protección en los delitos de daños informáticos tras las reformas de 2010 y 2015, esta controversia no parece que haya afectado a la cuestión que es objeto de atención aquí, pues un amplio sector doctrinal ha seguido admitiendo expresamente la punibilidad de los daños imprudentes[18]. También a esta conclusión parecen llegar otros autores a la vista de su forma de estructurar la explicación de los delitos de daños, todos ellos[19].

Parece que en apoyo de esta tesis ha tenido un gran papel, bien la opción seguida en torno al bien jurídico protegido, al mantenerse que es la propiedad o el patrimonio, bien la ubicación sistemática, porque esto supone que las ligaduras interpretativas de los delitos de daños no se rompen definitivamente[20], o porque tal ubicación sistemática afecta a la forma como ha de entenderse el bien jurídico, esto es, que se ha de dar un contenido patrimonial[21].

familiar (en el caso de los delitos tipificados en los arts. 197 bis y 197 ter), o el patrimonio, bien jurídico protegido en el art. 264.1 CP. Recurren a otras caracterizaciones del bien jurídico protegido en los daños informáticos, en todo caso no se trata de la protección de un bien jurídico de índole patrimonial, BARDAVÍO ANTÓN, 2020, pp. 408 s., refiriéndose al bien jurídico protegido a través de los ciberdelitos; GUÉREZ TRICARICO, 2021, nm. 11657/(p. 1414).

[18] Desde la protección del patrimonio, FERNÁNDEZ TERUELO, 2011, p. 105; ESTRADA CUADRAS, 2016, nm. 4629, 4635, 4694/(pp. 520 s., 521, 527 s.), admitiendo también la punibilidad de la participación imprudente en el delito de daños informático. Como ejemplo de participación imprudente cita el caso del programador de un virus que lo construye con una determinada potencialidad y este adquiere otra distinta por la intervención de un tercero; de los resultados que no ha previsto como consecuencias posibles del virus el programador no responderá dolosamente, pero sí imprudentemente, como autor o, generalmente, como partícipe, cuando de su intervención se derive una relación de incumbencia que le haga responsable de aquello que, posteriormente, otro realice o el mismo virus cause. Desde su ubicación sistemática, que no es la correcta, porque se tiene que proteger la seguridad informática, ANDRÉS DOMÍNGUEZ, 2011, pp. 430, 436. 441 s.; 2015b, p. 355, o es la integridad y disponibilidad de datos y sistemas informáticos, DE LA MATA BARRANCO, 2010, pp. 171 s., 174; 2016a, pp. 1092 s., 1095, 1097 s., 1098, 1105, 1106; 2018, pp. 743 s., 755. Desde la protección de un nuevo bien jurídico verdaderamente autónomo, la seguridad informática, no identificable con el patrimonio (ni con la intimidad), admiten la comisión imprudente RODRÍGUEZ MESA, 2017, p. 115; Sobre este bien jurídico, GIL GIL, 2021, pp. 485. También desde la protección de un nuevo bien jurídico ha de incluirse a LÓPEZ MUÑOZ, 2020, pp. 23 y ss., 77, porque sí propone un nuevo bien jurídico protegido por los ciberdelitos, aunque más adelante en la explicación del delito de daños informático no queda tan clara esta posición (p. 72). Aunque no aclara cuál es el bien jurídico protegido, pero se deduce que sí reconoce la aparición de uno nuevo surgido de los avances tecnológicos, por su comentario sobre la Decisión Marco 2005/222/JAI, y porque reclama un cambio en la ubicación sistemática de los daños informáticos, admitiendo a continuación su comisión imprudente ROMEO CASABONA, 2012, pp. 342, 369 n. 75, 370 (= 2013, pp. 624, 651 s. n. 75, 653).

[19] Véase, en este sentido, ORTS BERENGUER, 2019, pp. 501 y ss., 504; y reconociendo que los daños informáticos son delitos especiales, MORENO ALCÁZAR, 2020, pp. 375 y ss., 382 s., 385; MESTRE DELGADO, 2021a, pp. 443, 445, 448 s., 450 s.; ZUGALDÍA ESPINAR, 2021, pp. 313 y ss.

[20] Expresión utilizada por ANDRÉS DOMÍNGUEZ, 2010, p. 293; 2011, p. 430, añadiendo que tales ligaduras interpretativas son de difícil encaje en los daños informáticos; 2015a, p. 549; 2015b, pp. 352 s., 355. También se expresa en este sentido ESTRADA CUADRAS, 2016, nm. 4629/(p. 520 s.), reconociendo también que pueden ser de difícil encaje si se pretende responder a las distintas formas de sabotaje informático. Más adelante advierte que, en tipificación de los ataques de denegación de servicios, no resulta tan evidente su ubicación sistemática, dada la naturaleza plural de los intereses que se pueden ver afectados, en concreto, no se toma en consideración la afectación a la libertad de emisores y receptores de los servicios que se ofrecen a través de las TIC`s.

[21] Véase, en este sentido, DE LA MATA BARRANCO, 2010, pp. 159, 160, 165; 2016a, pp. 1092 s., 1095, 1097 s., 1098, 1100 y ss., 1105; 2018, pp. 742, 743 s., 755.

3. *Argumentos a favor de la punibilidad de los daños informáticos imprudentes*

En apoyo de la tesis a favor de la punibilidad de los daños informáticos imprudentes se pueden alegar varios argumentos, de manera individual o cumulativamente.

Un primer argumento, ya superado, se podía basar en la naturaleza del antiguo delito de daños informático, desde la hipótesis de que era un tipo cualificado o agravado del delito de daños. Y, en su refuerzo, también se podía tomar en consideración la literalidad de los diferentes preceptos reguladores de los delitos de daños, a saber, el del tipo básico (art. 263), el de los daños informáticos (antiguo art. 264.2) y el regulador de los daños imprudentes (art. 267).

Desde la primera perspectiva, la construcción como tipo cualificado de daños no sería un obstáculo para su punibilidad en la modalidad imprudente, pues ni los elementos fundamentales del delito de daños, ni los elementos adicionales que conforman el tipo derivado cualificado de daños informático[22], ninguno de ellos exige la actuación con intención o propósito específico que sea incompatible con la actuación imprudente. A mayor abundamiento, si el delito de daños informático era un tipo cualificado, esto significaba entonces que sí era elemento típico la superación de la cuantía económica[23] requerida en aquel momento para el delito de daños doloso, y su cuantificación se había de hacer, *a priori*, recurriendo a los mismos parámetros utilizados en el tipo básico (diferenciando entre los conceptos daño, para fijar la responsabilidad penal, y perjuicio, término utilizado para establecer la responsabilidad civil); si la modalidad dolosa se construía tomando en consideración el daño evaluable económicamente, y superando una determinada cuantía, ningún obstáculo habría para admitir la punibilidad de la comisión de los daños informáticos imprudentes,

[22] Sobre las clasificaciones de los tipos penales, por su relación con otros tipos, distinguiendo entre tipo básico/tipo agravado, que puede ser cualificado-privilegiado o autónomo, LUZÓN PEÑA, 2016, pp. 164 s.

[23] El requisito de la superación de la cuantía económica fijada para el delito de daños del art. 263 ha sido exigido por algunos autores que han reconocido que el antiguo delito de daños informático era un delito autónomo o especial, no un mero tipo agravado de daños. V., entre otros, GONZÁLEZ RUS, 1999, p. 6; 2002, pp. 1292, 1298; 2005a, pp. 789 s.; 2005b, p. 1476; 2006, p. 258; DE LA MATA BARRANCO, 2007, pp. 49 s., 51, si bien prescinde ya de la cuantía económica en DE LA MATA/HERNÁNDEZ, 2009, pp. 338, 340, 348; 2010b, pp. 226, 228, 235. Y desde la hipótesis de que el antiguo delito de daños informático era un tipo agravado, GARCÍA ARÁN, 2004, pp. 930 s.; FERNÁNDEZ TERUELO, 2007, pp. 112 s., 114; 2010, p. 251. Desde la actual regulación, QUERALT JIMÉNEZ, 2015, pp. 680, 683 s., partiendo del tenor literal del art. 264, donde no se establece una cuantía para la delimitación penal del hecho, en su lugar se exige que se produzca un resultado grave (y que las conductas también alcancen esta entidad), recurre a una interpretación sistemática con otros delitos patrimoniales con los que puede haber alguna similitud comparando las conductas, por eso selecciona los delitos de apoderamiento y descarta los de defraudación. Con este criterio hermenéutico, la cuantía económica en los daños informáticos del art. 264.1 será una cantidad que supere 20 veces la de 400 euros, en total 8.000 euros, una cifra que está por debajo de la cifra que la jurisprudencia utiliza para el hurto agravado (12.000 euros). Y en el comentario al art. 264 bis.3 CP afirma que, por razones sistemáticas y de proporcionalidad, aquella cifra se ha de incrementar en un 50%, llegando así a los 12.000 euros. Otra es la cuantía utilizada por GONZÁLEZ CAMPO, 2018, p. 432, quien también recurre a la interpretación jurisprudencial del hurto agravado, pero fija la cuantía en 50.000 euros. Esta última cifra es la que utiliza como referencia ESTRADA CUADRAS, 2016, nm. 4702/(p. 528 s.), para la interpretación del tipo agravado del art. 264.2 CP.

primero, porque este también requiere la superación de una cuantía económica; segundo, porque para la cuantificación de los daños también aquí se distingue entre el concepto de daño, relevante penalmente, y el de perjuicio, a tomar en cuenta para la responsabilidad civil.

Porque, a mayores, como ya se ha avanzado, a favor de la punibilidad de los daños informáticos imprudentes también se podía utilizar el tenor literal; en el art. 267 se describía -y se mantiene así en la actualidad- la conducta típica como "los daños causados" por imprudencia grave; en el antiguo art. 264.2 una de las conductas típicas era "de cualquier otro modo dañe"; alternativamente se mencionaban otras conductas típicas (destruir, alterar, inutilizar) que podían ser entendidas como especificaciones o modalidades de la genérica "dañar".

Con las reformas de 2010 y 2015 este argumento, en esos mismos términos, ya no puede mantenerse. Pero sí cabe el recurso a otro tipo de consideraciones, que también podían ser alegadas con anterioridad.

Así, el segundo argumento, y principal, que podría esgrimirse a favor de la punibilidad de los daños informáticos imprudentes es el relativo a la ubicación sistemática y, en conexión con ella, a la propia estructura del Capítulo en el que aparecen reguladas estas figuras delictivas.

Como ya se ha mencionado, los daños informáticos están ubicados en el Capítulo IX, que lleva por rúbrica "de los daños". Su estructura es como sigue: en primer lugar, ocupando los arts. 263 a 266, se describen las diferentes modalidades de daños cometidas dolosamente, entre las que se cuentan los acabados de citar; cerrando el Capítulo aparece el art. 267, precepto dedicado a los daños cometidos con imprudencia grave (y superando una determinada cuantía). Además, en su redacción se alude de manera genérica a los daños, el mismo concepto usado para dar nombre al Capítulo, con dos únicas limitaciones referidas, por un lado, a la superación de una determinada cuantía, y, por otro lado, a que la imprudencia sea grave. No se hace ninguna otra restricción referida a alguna de las modalidades típicas descritas con carácter previo. Se puede entender, entonces, que este precepto actúa a modo de cláusula genérica de tipificación de los daños imprudentes, cuando la imprudencia sea grave y la cuantía del daño causado supere la cifra establecida legalmente, sea cual sea la clase de objeto dañado y/o las circunstancias que eventualmente puedan concurrir. Solo si de la construcción de alguna de las modalidades típicas se deduce claramente que se limita su incriminación a título de dolo quedará excluida en tal caso del ámbito aplicativo de esta cláusula general incriminadora de los daños imprudentes. La duda se plantea de manera específica en aquellas modalidades delictivas que literalmente exigen la actuación con una determinada intención o propósito, o, dicho de otra manera, cuando nos encontramos ante delitos con especiales elementos subjetivos del injusto, ya que en estos casos se ha de analizar con detenimiento si tales elementos

subjetivos son o no compatibles con la comisión imprudente[24]. En concreto, se podría entender que sí se está incriminando solo la comisión dolosa, por ejemplo, en el tipo cualificado de daños del art. 263.2, en relación con la circunstancia cualificante referida a que se causen daños para impedir el libre ejercicio de la autoridad. O, en los daños informáticos, la modalidad prevista en el art. 264 ter, pues las conductas aquí descritas han de realizarse con la intención de facilitar la comisión de alguno de los delitos de los arts. 264 o 264 bis. En este último caso habría una razón más para concluir que queda fuera de la incriminación de la imprudencia: en realidad el art. 264 ter está incriminando actos preparatorios de los delitos de daños informáticos, así que, si esta es su verdadera naturaleza, su tipificación ha de quedar limitada a la comisión dolosa. Porque, por otro lado, si en este precepto se incriminan actos preparatorios de los daños informáticos, esto ha de significar que con su comisión aún no se ha cometido un daño cuantificable económicamente, sean cuales sean los parámetros utilizados para hacer este cálculo, así que mal podrá superarse la cuantía económica exigida para la aplicación del delito de daños imprudente.

Al argumento de la ubicación sistemática/estructura del Capítulo se puede recurrir al margen de la discusión teórica sobre el objeto de protección en los daños informáticos. Así se ha podido constatar en el apartado anterior dedicado a la postura doctrinal a favor de la punibilidad de los daños informáticos imprudentes. Evidentemente, para la tesis que sostiene que el bien jurídico protegido es el patrimonio, o más específicamente, la propiedad, la conclusión de que también los daños informáticos imprudentes son punibles es más que lógica. También, en parte, se puede llegar a esta deducción si, por la ubicación sistemática, se interpretan los daños informáticos en clave económica, aunque se reconozca que el objeto de interés no es estrictamente (o, en su caso, exclusivamente) el patrimonio. No lo es tanto para los partidarios de la protección de un nuevo bien jurídico vinculado a las TIC`s, a no ser que, por la relevancia de este novedoso bien jurídico, resulte justificada la intervención penal para su protección ante conductas dolosas o imprudentes que lo lesionen y/o lo pongan en peligro. Sobre esta cuestión se volverá después; desde la última de las tesis, el mero hecho de que la ubicación sistemática es la que es no debería ser el aspecto a tener en cuenta, el único en la práctica, para apoyar la punibilidad de los daños informáticos imprudentes. Con más motivo aún si en la explicación del bien jurídico se opta por la aceptación de que se defiende un nuevo bien jurídico, colectivo o supraindividual, la seguridad informática, y se prescinde de las ligaduras interpretativas de los delitos de daños, esto es, la valoración del grave daño en datos o programas

[24] Sobre la compatibilidad o no de la comisión imprudente en delitos con especiales elementos subjetivos del injusto, véase, por todos, LUZÓN PEÑA, 2016, p. 225. En el caso de los delitos de daños, sí ha de ser objeto de estudio la compatibilidad DE determinadas modalidades delictivas de daños con la comisión imprudente, dada la forma como se ha tipificado el delito imprudente, cerrando el Capítulo IX, exigiendo como requisitos típicos que se causen daños superando una determinada cuantía y que la imprudencia sea grave, sin más especificaciones.

informáticos o documentos electrónicos/grave obstaculización del funcionamiento del sistema informático no se mide por las consecuencias económicas que se derivan, sino que el grave daño/grave obstaculización ha de valorarse desde la afectación a la integridad y/o LA disponibilidad de datos y/o sistemas informáticos[25]. Si esto se hace así para los daños informáticos dolosos, entonces difícilmente se puede recurrir al art. 267 para castigar los daños informáticos imprudentes, pues esto significa ni más ni menos interpretar de manera diferente los elementos típicos dependiendo de si se está ante un delito doloso (no es relevante la cuantía económica, solo importa el grave daño a la integridad y/o disponibilidad del dato o del sistema informático) o si se está ante un delito imprudente (aquí sí se tiene que hacer una valoración económica del grave daño al dato o al funcionamiento del sistema informático, ya que tiene que superar la cuantía de 80.000 euros).

Un último argumento, que no sirve sin embargo de justificación, consistiría en que con la punibilidad de los daños informáticos imprudentes se pueden evitar interpretaciones forzadas sobre el dolo. O, a la vista de la redacción de los arts. 264 y 264 bis, en particular en relación con las circunstancias cualificantes de primer y segundo nivel (arts. 264.2 y 3 y 264 bis.1 párrafo segundo y apartado dos respectivamente) en menor medida respecto de la circunstancia cualificante de tercer nivel (arts. 264.3 y 264 bis.3), para evitar la interpretación de estas figuras delictivas como delitos cualificados por el resultado. Para ilustrar este riesgo sirva como ejemplo la forma como se presentan a veces los casos que se mueven entre el dolo eventual y la imprudencia: el caso de introducción de órdenes que provocan su autorreproducción y el resultado final escapa al control o previsión del sujeto activo[26]; o el caso del sujeto que tiene dolo de causar un daño de una determinada gravedad y va más allá de lo previsto; hay dolo eventual respecto de este daño más grave, solo en casos puntuales se habrá de recurrir al delito imprudente[27]. O cuando el autor introduce un virus en la red y desconoce si va a afectar efectivamente a algún usuario informático, o a qué tipo de datos o programas va a hacerlo; en este tipo de casos no habrá problema para plantear que existe al menos dolo eventual[28]. Debe aclararse que se trata de ejemplos planteados de manera muy genérica, simplemente para dejar constancia de que estos delitos admiten su comisión con dolo eventual o de manera imprudente, en ningún momento se está afirmando que estos autores están realizando una interpretación

[25] Esta es la tesis de RODRÍGUEZ MESA, 2017, pp. 65 s., 74 y ss., 78 s., 93: partiendo de que el bien jurídico es la seguridad informática, concretado en los daños informáticos en la protección de la integridad y disponibilidad de datos y sistemas informáticos, en la interpretación del resultado de daño grave en los datos o de grave obstaculización en el funcionamiento del sistema informático este se ha de fijar sin acudir al valor económico, sino a la gravedad de la pérdida de funcionalidad, tomando en consideración parámetros como la naturaleza, el contenido, la cantidad de los objetos afectados, la permanencia o la reversibilidad y la duración del ataque.

[26] ANDRÉS DOMÍNGUEZ, 2009, p. 422; 2011, pp. 441 s.; 2015b, p. 355.

[27] DE LA MATA BARRANCO, 2010, p. 171; 2016a, p. 1105; 2018, pp. 755 s.

[28] DE LA MATA BARRANCO, 2018, pp. 755 s.

como la denunciada. Es más clarificadora, porque es más detallada, la referencia a que sí hay dolo en el caso del sujeto que introduce un virus en el sistema informático o en la red sin saber a cuántos usuarios en concreto va a acabar dañando, pero el sujeto que introduce el virus sí conoce la potencialidad de su comportamiento respecto del eventual resultado que se le va a atribuir, esto puede afirmarse en el caso del sujeto que programa la propagación del virus a través del correo electrónico[29], es decir, es conocedor (y lo asume) de que, por la dinámica comisiva, el virus puede causar un daño grave en el sistema que va a afectar y, además, puede afectar a tantos sistemas como sean alcanzados por el virus si no se han adoptado medidas de seguridad que lo detecten y lo bloqueen y/o desactiven.

En ocasiones se pueden plantear supuestos de preterintencionalidad, esto es, el sujeto actúa con dolo de causar daños informáticos a una determinada persona, pero acaba causando un daño mayor, o causa daños a otra u otras personas y estos resultados más graves o ulteriores ya no están abarcados por el dolo, pero sí son imputables a la imprudencia. Para los partidarios de la punibilidad de los daños informáticos imprudentes la solución a estos casos pasa por la aplicación de las reglas del concurso de delitos, si se cumplen los requisitos típicos (sobre todo del delito imprudente, se supera la cuantía económica) entre el delito de daños informático doloso y el/los delitos informáticos imprudente/s[30], solución respetuosa con el principio de responsabilidad subjetiva (art. 5 CP). De descartarse la punibilidad de los daños imprudentes, para casos como estos la solución habrá de pasar por castigar solo los daños causados dolosamente, quedando sin sanción penal los imputables a la imprudencia del sujeto; otra solución sería contraria al citado principio de responsabilidad subjetiva.

Una vez admitida la punibilidad de los daños informáticos imprudentes, se entra en dos problemas no sencillos de resolver: en primer lugar, porque el art. 267 exige que los daños superen la cuantía de 80.000 euros, por lo que será preciso decidir de qué manera se ha de valorar el daño causado. O, dicho de otra manera, qué parámetros se han de tomar en consideración para la cuantificación del daño informático a efectos penales[31]. Este es un problema que ya se plantea en la interpretación de los

[29] ESTRADA CUADRAS, 2016, nm. 4692/(p. 527).

[30] Plantean este concurso ideal entre los daños informáticos dolosos y los daños imprudentes, RODRÍGUEZ/ALONSO/LASCURÁIN, 2001, p. 285; GONZÁLEZ RUS, 2005a, p. 797; 2005b, p. 1484; 2006, p. 269; DE LA MATA/HERNÁNDEZ, 2009, p. 350; 2010b, pp. 237 s.; DE LA MATA BARRANCO, 2010, pp. 171 s., 174; 2016a, p. 1105; 2018, p. 756.

[31] DE LA MATA BARRANCO, 2016a, pp. 1100, 1105; 2018, p. 756, para la interpretación de la cuantía en los daños imprudentes propone que se tome en cuenta la forma como se interpreta el concepto grave en los delitos dolosos. Los tipos agravados de daños informáticos ya están dando pautas interpretativas. RODRÍGUEZ MESA, 2017, p. 115, hace la siguiente propuesta en la interpretación: en los daños informáticos no ha de existir necesariamente un menoscabo patrimonial, ya que para esta autora el bien jurídico protegido no se ha de interpretar en clave patrimonial. Ahora bien, en los daños informáticos imprudentes sí es necesario que se cumpla el requisito de que el daño supere la cuantía de 80.000 euros. Así que en la cuantificación del daño incluye el perjuicio del hecho delictivo.

daños dolosos: por mencionar solo los tipos básicos, hay que decidir cuándo el daño en datos, programas informáticos o documentos electrónicos es grave (art. 264) o la interrupción o la obstaculización del funcionamiento del sistema informático es grave (art. 264 bis). En segundo lugar, se ha de determinar cuándo la imprudencia cometida por el sujeto es grave.

Dando por hecho que se cumple el primer requisito (se supera la cuantía de 80.000 euros), se ha de decidir si ha de calificarse como imprudencia grave la cometida por el sujeto que reenvía a otros con conocimiento un correo sospechoso de contener un virus que, finalmente, sí infecta a otros usuarios a los que no hubiera llegado sin su intervención[32]. O la del sujeto que distribuye archivos de procedencia dudosa sin haber analizado previamente su peligrosidad[33].

III. **En contra de la punibilidad de los daños informáticos imprudentes**

1. ***La opinión doctrinal***

Aunque minoritario, un sector de la doctrina ha descartado de manera (más o menos) expresa la punibilidad de los daños informáticos cometidos imprudentemente, no siempre utilizando los mismos argumentos, como se va a mencionar a continuación.

Esta declaración expresa se ha formulado sobre todo en comentarios hechos tras las reformas legislativas de 2010 y 2015, si bien algún autor ha defendido esta postura con la antigua regulación del delito de daños en el antiguo art. 264.2, como se va a ver enseguida.

En ocasiones se ha llegado a esta conclusión tomando en consideración la explicación del precepto regulador de los daños imprudentes (art. 267), en concreto, porque este se pone en relación con el delito de daños del art. 263 CP[34], y, a veces, además, se ha reconocido que los delitos de daños informáticos son delitos especiales

[32] Es el ejemplo de ESTRADA CUADRAS, 2016, nm. 4694/(p. 528). Este autor aclara que es necesario que sea el sujeto el que reenvíe el virus a otros usuarios, pues es algo normal que el usuario que recibe un virus desconozca que el mismo se ha enviado a todas las direcciones contenidas en su *libreta* de correo electrónicos; en estos casos, cuando no es el usuario el que reenvía el correo infectado no se le exigirá responsabilidad penal alguna.

[33] Ejemplo propuesto por DE LA MATA BARRANCO, 2018, p. 756, aclarando que, para este supuesto pudiera ser suficiente con la reparación en sede civil.

[34] DE URBANO CASTRILLO, 2007, p. 2125; QUERALT JIMÉNEZ, 2015, pp. 681, 685; MADRIGAL/LANZAROTE, 2018, pp. 1593, 1600. Por su parte, MORÓN LERMA, 2002, p. 67, si bien ha admitido la punibilidad de los daños informáticos imprudentes, ha añadido sin embargo que no parece que la producción de daños informáticos imprudentes "fuese la realidad que el legislador quería encauzar normativamente".

o autónomos, con una ubicación incorrecta[35], de lo que se deduce que no están orientados a la protección de un bien jurídico de carácter patrimonial, pero también se ha seguido manteniendo que se está en presencia de delitos patrimoniales[36].

Otras veces parece que el argumento utilizado ha sido el relativo al bien jurídico protegido en los delitos de daños informáticos. Pese a su ubicación sistemática, en estos delitos no se está protegiendo el patrimonio, o la propiedad; se está en presencia de un nuevo bien jurídico surgido con el desarrollo de la informática y las TIC's que necesita ser garantizado a través del DP, sea este la seguridad informática, sea la integridad y disponibilidad de los datos y sistemas informáticos[37]. De tal argumento se deduce, entonces, que al menos los ciberdelitos puros o en sentido estricto solo admiten la comisión dolosa, y, por otro lado, el precepto penal que incrimina la imprudencia se ha de conectar con los delitos de daños en sentido estricto.

Por último, en apoyo de esta tesis se ha alegado que en el art. 264 (y lo mismo sucede en el art. 264 bis) se castiga el daño grave, con un doble requisito de gravedad, referido a la conducta típica y al resultado causado, así que no se contemplan modalidades imprudentes de comisión[38].

[35] DE URBANO CASTRILLO, 2007, p. 2125. Este autor, en 2012, p. 28, sí afirma que en los daños informáticos se protege más la integridad del sistema que el patrimonio, lo que además debería suponer un replanteamiento de su estructura típica, en concreto, debería ser formulado como un delito de consumación anticipada. También MORALES GARCÍA, 2012, p. 159, defiende la tipificación de los daños informáticos siguiendo la estructura de los delitos de consumación anticipada, una postura que ya había propuesto en 2010, pp. 188 s., añadiendo que, con esta técnica legislativa, el bien jurídico se desplazaría desde el patrimonio hasta la integridad del sistema, en la línea de la política criminal internacional y de la Decisión Marco 2005/222/JAI.

[36] QUERALT JIMÉNEZ, 2015, pp. 447 y ss., 678 y ss., porque ubica todos los delitos de daños en la sección dedicada a los delitos contra los valores patrimoniales individuales (en esta sección explica, entre otros, los delitos de hurto, robo, estafa, apropiación indebida); MADRIGAL/LANZAROTE, 2018, p. 1593.

[37] CÁMARA/CANO/GARCÍA/GIL (coord.)/HERNÁNDEZ (coord.)/MARTÍN/PASTOR/ROBLES/TOBARRA, 2019, pp. 148 y ss., 161 y ss., 218; apoyan la existencia de un nuevo bien jurídico, la seguridad informática, con un doble contenido, por un lado, se trata de adelantar las barreras de protección de otros bienes jurídicos, individuales, colectivos y, en particular, la información, y, por otro lado, tiene una dimensión positiva, garantizar las condiciones necesarias para el correcto funcionamiento de la sociedad en el ámbito de las TIC. Estos autores hacen referencia a los conceptos estricto o amplio de ciberdelitos: al primer grupo, en el que se engloban los daños informáticos, pertenecen los delitos que atentan contra la integridad, la disponibilidad y la confidencialidad de redes y sistemas informáticos (p. 156). Critican la ubicación sistemática de los delitos de daños informáticos, añadiendo que esta incorrecta ubicación lleva a la incomprensión e injustificada crítica por una parte de la doctrina que trata de interpretar estas figuras delictivas en función de la ubicación sistemática (p. 177). Reconoce que los daños informáticos protegen un nuevo bien jurídico, la integridad y disponibilidad de datos y sistemas informáticos, BARRIO ANDRÉS, 2012, pp. 39 y ss., 42 y ss. Este puede ser el argumento que ha podido llevar a este autor a concluir que los daños informáticos solo se pueden cometer dolosamente en 2018, pp. 107 y ss., 113. También puede ser este el argumento utilizado por GONZÁLEZ CAMPO, 2018, pp. 429, 430 y ss., partiendo del bien jurídico protegido la integridad y disponibilidad de datos y sistemas informáticos (si bien reconoce que el art. 264 es un delito contra el patrimonio y en el art. 264 bis considera como bien jurídico el buen funcionamiento de los sistemas interconectados o redes).

[38] Es el argumento esgrimido por VELASCO NÚÑEZ, 2019, p. 51. A la misma conclusión parece llegar HERRERO-TEJEDOR ALGAR, 2011, p. 153.

2. *Otros argumentos en contra de la punibilidad de los daños informáticos imprudentes*

A la conclusión descartando la punibilidad de los daños informáticos imprudentes se puede llegar recurriendo a varios argumentos, que también pueden presentarse de manera cumulativa. Algunos han sido utilizados por este sector doctrinal minoritario, si bien conviene hacer una explicación algo más detallada.

En primer lugar, se puede utilizar el argumento literal, haciendo una previa comparación entre la forma como se han descrito los delitos de daños de los arts. 263.1 y 2/267, por un lado, y los daños informáticos de los arts. 264 y 264 bis (y 263 ter y quater), por otro lado. En el primer grupo se ha utilizado la misma técnica para describir la conducta típica, genéricamente como "el que causare daños" o "los daños causados por imprudencia grave", en el segundo grupo el legislador ha optado por otra fórmula descriptiva. Además, en el primer grupo se ha establecido como requisito típico la cuantificación económica de los daños causados en cosa ajena, elemento eliminado en los daños informáticos[39], en su lugar el legislador ha recurrido a una descripción indeterminada, que los daños (y similares) en datos sea grave/la interrupción o la obstaculización del sistema sea grave. Derivado del recurso a la cuantía económica, en los delitos de daños la cuantía sirve para establecer la distinción entre delito leve-delito menos grave (en el delito doloso), pero en cualquier caso el daño en cosa ajena, sea cual sea la cuantía de ese daño, es penalmente relevante siempre, con la limitación que resulte en todo caso de la aplicación del principio de insignificancia como causa de atipicidad penal[40]. En los daños informáticos se ha optado por la eliminación del recurso a la cuantía económica, en su lugar se exige que el resultado causado sea grave, de lo que resulta que, en los casos en los que el daño resultante no alcance esta calificación, el hecho será atípico penalmente[41].

[39] Desde las reformas de 2010 y 2015, casi de manera unánime, la doctrina ha entendido que la aplicación de los delitos de daños informáticos no depende de la superación de una determinada cuantía, entre otras razones porque no se ha hecho referencia alguna en su redacción. V., entre otros, ANDRÉS DOMÍNGUEZ, 2011, p. 433; 2015b, p. 353; RAGUÉS/ROBLES, 2012, p. 374; ROMEO CASABONA, 2012, p. 370 (= 2013, p. 653); DE URBANO CASTRILLO, 2012, p. 24; RODRÍGUEZ MESA, 2017, pp. 63, 64; FERNÁNDEZ DÍAZ, 2018, pp. 14, 23; ECIJA, 2019, nm. 8250/(p. 720); BENÍTEZ ORTÚZAR, 2020, p. 662; LÓPEZ MUÑOZ, 2020, p. 76; GUTIÉRREZ (coord.)/CASTRO/PÉREZ, 2021, p. 55. También en la interpretación jurisprudencial se llega a esta misma conclusión. V., entre otras, la STS 22 mayo 2020 (ECLI:ES:TS:2020:1520); SAP SE 6 junio 2019 (ECLI:ES:APSE:2019:1497A); SAP LE 25 junio 2020 (ECLI:ES:APLE:2020:844). Ya con la antigua regulación del delito de daños informático (antiguo art. 264.2) un sector de la doctrina había descartado que fuera elemento típico la superación de una determinada cuantía económica (la cuantía fijada en el delito de daños del art. 263). V., entre otros, GUTIÉRREZ FRANCÉS, 1996, p. 298; FERNÁNDEZ/MORALES, 2000, p. 1527; MATELLANES RODRÍGUEZ, 2000, pp. 142 s.; MORÓN LERMA, 2002, p. 67; ANDRÉS DOMÍNGUEZ, 2009, p. 419; DE LA MATA/HERNÁNDEZ, 2009, p. 338; 2010b, pp. 228, 235; DE LA MATA BARRANCO, 2010, p. 165.

[40] Sobre el principio de insignificancia, su naturaleza jurídica como causa de atipicidad penal (entendida como exclusión solo de la tipicidad penal, pero sin que ello suponga que la conducta sea conforme a derecho, sigue siendo una conducta contraria a derecho, pero no está prohibida penalmente), LUZÓN PEÑA, 2016, pp. 319, 326 ss., 328 s., 40 s.

[41] Así lo afirman expresamente, entre otros, FERNÁNDEZ TERUELO, 2011, p. 99; BARRIO ANDRÉS,

Siguiendo con el argumento literal, ahora tomando en consideración el resto de los delitos de daños, por un lado, y los daños informáticos, por otro lado. Cierto es que en el art. 265 no se ha recurrido solo al verbo genérico de dañar o causar daños en los objetos enumerados en este precepto, pues también se han añadido los verbos destruir, que es sinónimo de este, e inutilizar, que permite abarcar comportamientos que quedarían fuera de los verbos destruir y dañar, para el caso de que estos se interpreten referidos al menoscabo de la sustancia de la cosa[42], pero sí se ha recurrido al otro elemento descriptivo, la cuantificación económica del "daño" en los objetos, medios, instalaciones al servicio de las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad. Ahora bien, ese verbo, o más exactamente el sustantivo "daño" sí se ha utilizado en el art. 266: aquí se alude literalmente a cometer los "daños" que aparecen descritos en los arts. 263.1, 263.2, 265 (y, además, en los arts. 323 y 560), y ya no hay remisión a los daños informáticos desde la reforma del art. 266 operada por la LO 1/2015[43].

En resumidas cuentas, de esta comparativa resulta que el Capítulo IX lleva por rúbrica "de los daños", y este es el término utilizado en los arts. 263, 265 y 266, no en los daños informáticos. Así que en la interpretación del art. 267, que también se utiliza el término daños en su redacción, este se ha de poner en conexión o relación con los daños de los arts. 263, 265 y 266.

Como se ha mencionado, en la descripción de los delitos de daños, incluido el art. 267, se recurre a la cuantificación económica del objeto o cosa dañada como elemento típico; la acción es dañar, el resultado es causar daños; todos estos elementos

2012, p. 44; 2016, p. 13; 2018, p. 112; RAGUÉS/ROBLES, 2012, p. 374; ROMEO CASABONA, 2012, p. 370 (=2013, p. 653), explicando también las diferentes respuestas penales que podrían plantearse de recurrir a los delitos menos grave y leve de daños del art. 263 si aquí se subsumieran los daños informáticos que no alcancen la consideración de graves (y en la interpretación del término grave se usa como referencia la cuantía económica de 400 euros, pero sin que se identifique con esta cuantía); CORCOY BIDASOLO, 2015, p. 934; 2019, p. 581; QUERALT JIMÉNEZ, 2015, p. 681; ESTRADA CUADRAS, 2016, nm. 4635, 4674/(pp. 521, 526); MANZANARES SAMANIEGO, 2016, p. 961; RODRÍGUEZ MESA, 2017, p. 78; CÁMARA/CANO/GARCÍA/GIL (coord.)/HERNÁNDEZ (coord.)/MARTÍN/PASTOR/ROBLES/TOBARRA, 2019, pp. 217 s.; GIL GIL, 2021, p. 484; SERRANO TÁRRAGA, 2021, p. 267. Parece defender esta misma interpretación DE LA MATA BARRANCO, 2010, p. 165; 2016a, p. 1100. Más allá va GORJÓN BARRANCO, 2021, pp. 104, 111, 120, al proponer que la intervención penal se debería limitar aún más: solo a los supuestos que hoy forman parte de los tipos cualificados de daños informáticos, los daños subsumibles en los tipos básicos de los arts. 264.1 y 264 bis.1 (párrafo primero) deberían quedar fuera del DP. A la misma conclusión sobre la atipicidad penal si los daños informáticos no alcanzan el calificativo de grave se llega en la STS 22 mayo 2020 (ECLI:ES:TS:2020:1520).

[42] Sobre la interpretación de las conductas típicas del art. 265, v., por todos, ANDRÉS DOMÍNGUEZ, 1999b, pp. 216 s.; 2011, p. 438; 2015b, p. 368; GARCÍA ARÁN, 2004, p. 933; CORCOY BIDASOLO, 2015, p. 938; 2019, p. 576; RODRÍGUEZ MESA, 2017, pp. 105 s.

[43] En la versión originaria del vigente CP el art. 266 se limitaba a castigar más gravemente los daños descritos en el art. 265 cometidos recurriendo al incendio, o un medio capaz de causar estragos o que ponga en peligro la vida o integridad de las personas. El art. 266 es objeto de una primera reforma a través de la LO 7/2000, de 22 de diciembre; en este momento se opta por la ampliación de la aplicación de este precepto para castigar los daños previstos en los arts. 263, *264*, 265 (y 323 y 560) cuando se cometan utilizando medios de gran potencialidad destructiva y/o peligrosos para las personas. El art. 266 se modifica por segunda vez en el año 2015, para excluir de su ámbito de aplicación los daños informáticos.

se pueden interpretar restrictivamente, atendiendo al valor económico de la cosa, o ampliamente, abarcando también el valor de uso (porque así también se interpreta el propio bien jurídico protegido), en todo caso el concepto de daño es diferente y más restrictivo que el de perjuicio[44]. No sucede así en los daños informáticos. Y, además, el término que en ocasiones se utiliza para la descripción de los daños informáticos, en concreto en algunas de las circunstancias cualificantes, es el de perjuicio, no el de daño. O, visto desde la responsabilidad penal de las personas jurídicas, el concepto "perjuicio" es el que se ha de tomar en consideración para todas las modalidades típicas de los daños informáticos, sean los tipos básicos, sean los tipos cualificados de primer, segundo o tercer nivel. Si efectivamente se ha de distinguir entre daño y perjuicio, y el art. 267 establece como parámetro aplicativo la cuantificación del daño, sin tomar en consideración el perjuicio, entonces su ámbito aplicativo se tendrá que establecer desde los delitos de daños que requieren como elemento típico el daño causado, y tomando en cuenta las modalidades delictivas que también utilizan la cuantía económica para su descripción. Al delito de daños imprudente del art. 267 sí se tendrá que recurrir para castigar las conductas imprudentes que dañan los elementos físicos del sistema informático, sin afectar a su contenido (datos, documentos, programas) o a su funcionamiento. Este hecho no plantea ninguna especificidad respecto de los delitos "tradicionales" de daños, pues los elementos físicos también son cosas materiales o corporales susceptibles de deterioro en su sustancia y, si este es también un aspecto a valorar en la cuantificación del daño, en su funcionalidad[45].

Ahora bien, el argumento literal no es concluyente desde el momento en que en los daños informáticos también se recurre a los términos dañar o daño. Porque como verbo típico aparece dañar de manera grave en el art. 264.1; como formas de provocar la interrupción o la obstaculización del sistema informático se alude a dañar de manera grave datos o programas informáticos o documentos electrónicos o a destruir o dañar un sistema informático en el art. 264 bis.1; una de las circunstancias cualificantes de los arts. 264.2 y 264 bis.2 se refiere a ocasionar daños de especial gravedad. Por otro lado, como se ha visto anteriormente, en los delitos de daños no solo se recurre al verbo dañar para su descripción, es el caso de los daños tipificados en el

[44] Sobre esta diferenciación (y en la interpretación del término daño se puede recurrir a una interpretación restrictiva, atendiendo al daño en la sustancia de la cosa y a su valor económico, o amplia, abarcando el daño funcional y el valor de uso), v., entre otros muchos, ANDRÉS DOMÍNGUEZ, 1999b, pp. 141 s., 145 y ss.; 2011, pp. 423 s.; 2015b, p. 339; GARCÍA ARÁN, 2004, p. 924; MIRÓ LLINARES, 2010, nm. 1505-1506/(p. 163); CORCOY BIDASOLO, 2015, p. 928; 2019, p. 574; RODRÍGUEZ MESA, 2017, pp. 22, 23 y ss.; NIETO MARTÍN, 2019, p. 209; VELASCO NÚÑEZ, 2019, p. 53; MUÑOZ CONDE, 2021, pp. 451 s., 462.

[45] Ya con la antigua regulación del delito de daños informático se hacía la aclaración de que los daños en los elementos físicos-materiales o corporales-, cuando la conducta solo afectaba a estos, eran subsumibles en los daños "tradicionales", quedando reservado el delito de daños informático para los hechos que afectaban solamente a los elementos lógicos o a elementos lógicos y físicos si ambos son afectados por la misma conducta. Esta aclaración se sigue haciendo en la actual regulación. Para más detalles, v., por todos, GONZÁLEZ RUS, 2002, pp. 1281 y ss., 1288 y ss., 1295 y ss.; 2005b, pp. 1471 s., 1472 s., 1484; ANDRÉS DOMÍNGUEZ, 2009, pp. 416 s.; 2011, pp. 430 s.; DE LA MATA/HERNÁNDEZ, 2009, pp. 312 s., 316 y ss., 318 s.; 2010b, p. 263; RAGUÉS/ROBLES, 2012, p. 374; GUTIÉRREZ (coord.)/CASTRO/PÉREZ, 2021, p. 55.

art. 265 CP, donde las conductas típicas son dañar, destruir o inutilizar. Además, porque los delitos de daños no son solo los que aparecen en el Capítulo IX, pues, tal como se reconoce expresamente en el art. 263.1 CP, hay daños en propiedad ajena que están comprendidos en otros títulos del CP. Entre estos otros delitos que castigan los daños en propiedad ajena hay que citar el art. 560 CP, donde se castiga al que cause daños que interrumpan, obstaculicen o destruyan líneas o instalaciones de telecomunicaciones o la correspondencia postal, o interrumpan o alteren gravemente el suministro o servicio de agua, gas o electricidad; la similitud en especial con la redacción del art. 264 bis es más que evidente. Y porque, en última instancia, si se acaba reconociendo que los conceptos tradicionales de "daño" o del verbo "dañar" no son trasladables a estos ciberdelitos, porque tales términos han de entenderse como la destrucción o el deterioro de la sustancia de una cosa corporal o material, y/o porque para la cuantificación de los daños se ha de atender solo al valor económico de la cosa, no se ha de incluir el valor funcional de la misma, interpretaciones sobre las que no existe unanimidad, por otra parte, entonces, para salvar los posibles problemas derivados del principio de legalidad, lo que ha hecho el legislador en la redacción de los daños informáticos es describir todas las posibles conductas que, materialmente, han de entenderse que equivalen a la de dañar la sustancia de una cosa material cuando las mismas recaen sobre cosas inmateriales: si en una cosa material el daño en su sustancia repercute en su utilidad/funcionalidad, en los datos o programas informáticos, documentos electrónicos o sistemas informáticos, su utilidad/funcionalidad se ve afectada o menoscabada a través del borrado, el daño, el deterioro, la alteración, la supresión, la inaccesibilidad, en el primer caso, o la interrupción o la obstaculización de su funcionamiento, en el segundo caso. Y si en los daños en cosas materiales se puede recurrir solo al valor de la cosa en el mercado, en los daños informáticos el valor de mercado de los objetos materiales (datos, programas, documentos) no es el más importante, sino que lo es su valor funcional, al margen de los parámetros que se utilicen para darle contenido[46]. Y, finalmente, en los

[46] La gravedad del daño se puede calcular tomando en consideración el valor económico, desde una concepción funcional, bien porque así se deduce del bien jurídico objeto de protección, bien de la ubicación sistemática de estos delitos. V., en este sentido, entre otros, ANDRÉS DOMÍNGUEZ, 1999a, p. 1727; FERNÁNDEZ/MORALES, 2000, pp. 1524, 1527; MATELLANES RODRÍGUEZ, 2000, pp. 142 s.; MARCHENA GÓMEZ, 2001, pp. 358 s.; GARCÍA GONZÁLEZ, 2005, pp. 742, 778; DE LA MATA BARRANCO, 2007, pp. 51 s., si bien este autor en 2010, p. 165; 2016a, pp. 1097 s., 2018, pp. 750, 756, toma en consideración el perjuicio causado en la interpretación de estos delitos; DE LA MATA/HERNÁNDEZ, 2010a, p. 163; MIRÓ LLINARES, 2010, nm. 1485, 1505, 1510/(pp. 159, 163, 165); MORALES GARCÍA, 2010, p. 189; RAGUÉS/ROBLES, 2012, pp. 372 s.; ROMEO CASABONA, 2012, p. 368 (= 2013, p. 650); QUERALT JIMÉNEZ, 2015, pp. 679 s., incluyendo también el trabajo invertido en la incorporación de la información en los datos informáticos; ESTRADA CUADRAS, 2016, nm. 4658, 4662/(p. 524); FERNÁNDEZ DÍAZ, 2018, pp. 2, 10 s., 14 s., 16, 22 s.; BENÍTEZ ORTÚZAR, 2020, pp. 662 s.; ABADÍAS SELMA, 2021, p. 301; GORJÓN BARRANCO, 2021, p. 99; GUTIÉRREZ (coord.)/CASTRO/PÉREZ, 2021, p. 54; MUÑOZ CONDE, 2021, p. 462. Concretan algo más el concepto de daño desde la perspectiva funcional: se ha de tener en cuenta el valor en sí de los datos, su utilidad y el reflejo del menoscabo en la utilidad para el titular: ORTS/ROIG, 2001, pp. 81, 82, si bien advierten que desde esta lectura no se puede establecer con claridad la separación entre el daño y el perjuicio; ANDRÉS DOMÍNGUEZ, 2009, p. 419; 2011, pp. 433, 436;

delitos de daños informáticos también se puede establecer la distinción entre daño (grave, para que sea penalmente relevante, para la aplicación de los tipos básicos de los arts. 264.1 y 264 bis.1 CP) y perjuicio (para fijar la responsabilidad civil y la cualificación de primer, segundo y tercer nivel de los arts. 264.2, el último párrafo de este apartado y el apartado 3 y 264 bis.2 y 3 -porque los tipos cualificados se castigan con multa, atendiendo al perjuicio ocasionado)[47], al igual que sucede por

2015b, pp. 352 s. FERNÁNDEZ DÍAZ, 2018, pp. 15, 16, cita los siguientes parámetros, advirtiendo que no son los únicos: costes de recuperación de la información suprimida o alterada, relevancia que posee para la actividad empresarial, si la inutilización se produce por un periodo de tiempo en el que la empresa estaba cerrada, si la información es recuperable pero el daño es por tiempo suficiente como para generar una perturbación sustancial en la utilidad de los datos. AGUDO/JAÉN/PERRINO, 2018, p. 86; GUTIÉRREZ (coord.)/CASTRO/PÉREZ, 2021, p. 55; y SERRANO TÁRRAGA, 2021, pp. 364 s., se hacen eco de la interpretación de la jurisprudencia menor sobre los parámetros a utilizar para concretar si ha habido o no un daño grave: se tiene en cuenta el coste económico de la reparación o del perjuicio causado por la eliminación o inutilización, la posibilidad o no de recuperar los datos, la pérdida definitiva, la complejidad técnica de los trabajos de restauración, la duración de las tareas de recuperación o su coste. Para más detalles sobre la forma como se establece la gravedad del daño informático en la jurisprudencia menor véase, entre otras, SAP B 28 octubre 2016 (ECLI:ES:APB:2016:12899); SAP M 10 enero 2017 (ECLI:ES:APM:2017:480); SAP J 6 febrero 2018 (ECLI:ES:APJ:2018:131); SAP L 4 mayo 2018 (ECLI:ES:APL:2018:500); SAP BA 23 julio 2018 (ECLI:ES:APBA:2018:761); SAP SE 6 junio 2019 (ECLI:ES:APSE:2019:1497A); SAP LE 25 junio 2020 (ECLI:ES:APLE:2020:844). Estos parámetros también han sido los utilizados en la STS 22 mayo 2020 (ECLI:ES:TS:2020:1520). FERNÁNDEZ TERUELO, 2007, pp. 115 s.; 2010, p. 251; 2011, pp. 99 s., 101, descarta el recurso al valor funcional, por su proximidad al concepto de perjuicio. En su lugar propone que en la valoración de daño se atienda al coste de recuperación o restablecimiento de la información o del sistema, y se cometerá el delito si este no es recuperable o resulta muy difícil su recuperación. También advierte de la dificultad de diferenciar entre el daño y el perjuicio, con carácter general en los delitos de daños, y más complicado aún en los daños informáticos, MORENO ALCÁZAR, 2020, pp. 382 s., al considerar que son prácticamente coincidentes los daños valorados desde la perspectiva funcional y el perjuicio.

[47] Sí hacen la distinción entre daño y perjuicio DE LA MATA BARRANCO, 2007, pp. 51 s.; DE LA MATA/HERNÁNDEZ, 2010a, pp. 164 n. 8, 165, computando los perjuicios indirectos en la responsabilidad civil, también los perjuicios económicos que puedan derivarse de una deficiente producción de bienes de la empresa o de una incorrecta prestación de servicios; MIRÓ LLINARES, 2010, nm. 1485, 1505-6/(pp. 159, 163), interpreta los delitos informáticos atendiendo a su ubicación sistemática, por tanto, en clave patrimonial. El alcance de las conductas típicas se ha de valorar en sentido económico, aunque sea funcional. En responsabilidad civil computa los gastos ocasionados en la limpieza de los mensajes y los del nuevo sistema de protección instalado, también el lucro cesante; ESTRADA CUADRAS, 2016, nm. 4662, 4664/(p. 525), lleva a la responsabilidad civil el coste de la limpieza de los sistemas informáticos o el que conlleva la reconstrucción de datos y archivos, los relativos a la falta de funcionalidad del sistema afectado y el lucro cesante; MUÑOZ CONDE, 2021, p. 462; y BALEA ROUCO, 2021, pp. 4 s., también diferencian entre el daño, para la aplicación del delito de daños informáticos, y el perjuicio, para establecer la responsabilidad civil. Desde la interpretación del bien jurídico como seguridad de la información, desconectado de cualquier contenido o interpretación en clave patrimonial, RODRÍGUEZ MESA, 2017, p. 79, incluye en la responsabilidad civil el perjuicio causado, mencionando como parámetros a valorar en este los costes indirectos y la situación de desconfianza generada tras el ataque sufrido. Un sector de la doctrina propone que se recurra al concepto de perjuicio para la interpretación de los daños informáticos, sin distinguir por tanto entre los conceptos de daño y perjuicio. V., en este sentido, antes de la tipificación expresa del delito de daños informático en el CP, CORCOY BIDASOLO, 1990, pp. 1008 y ss., 1013 y ss., 1016 (=1992, pp. 160 y ss., 169 y ss., 175 s.); en la versión originaria de estos delitos, ÁLVAREZ VIZCAYA, 2001, pp. 274 y ss., 277; GONZÁLEZ RUS, 2007, p. 35, proponiendo también otra alternativa: para el tipo básico se ha de atender al daño económico del objeto, para los tipos cualificados el perjuicio causado. En la regulación actual ya toman en consideración el perjuicio causado, CORCOY BIDASOLO, 2015, p. 934; 2019, p. 581; BARRIO ANDRÉS, 2018, p. 112; NIETO MARTÍN, 2019, p. 216; LÓPEZ MUÑOZ, 2020, p. 75. Esta es la interpretación seguida también por CÁMARA/CANO/GARCÍA/GIL (coord.)/HERNÁNDEZ (coord.)/MARTÍN/PASTOR/ROBLES/TOBARRA, 2019, pp. 216 s., mencionando los siguientes parámetros

tanto en los delitos de "daños tradicionales", cuando para dar contenido al primer elemento se recurre al concepto de daño funcional.

Otro de los argumentos utilizados en defensa de la punibilidad de los daños informáticos imprudentes es el sistemático, unido a la forma como se estructura el Capítulo dedicado a los delitos de daños, dolosos e imprudentes. También se puede rebatir este razonamiento con la siguiente observación. Desde la reforma de 2010, completada con la de 2015, se ha establecido la responsabilidad penal de las personas jurídicas (tomando en consideración la terminología literal, sin entrar en la discusión de si es o no auténtica responsabilidad penal), siguiendo el sistema de *numerus clausus*. Por diferentes motivos que aquí no pueden ser desarrollados, se ha de entender que el legislador pretende establecer la responsabilidad de las personas jurídicas por delitos dolosos, a pesar de que atendiendo a la ubicación sistemática y estructura del capítulo donde se incardina el precepto regulador de esta responsabilidad puede generar alguna duda sobre la posible ampliación también a la comisión imprudente[48]. De esta manera se puede comprobar que el argumento sistemático no tiene que ser definitivo a la hora de establecer la exégesis de un determinado precepto penal. Porque si de la ubicación sistemática se tuviera que extraer una conclusión indiscutible, entonces tal deducción nos tendría que llevar también a la afirmación de la responsabilidad penal de las personas jurídicas por delitos informáticos imprudentes.

El argumento de mayor peso para llegar a la conclusión de que no se han de castigar los daños informáticos imprudentes es el que conecta con su carácter autónomo

para su valoración (citando en este particular la Circular FGE 3/2017, p. 53): el valor de la destrucción definitiva de los datos informáticos, el coste de restablecimiento de la operatividad de los datos, programas o, en su caso, del sistema, el perjuicio económico que haya supuesto para el afectado el periodo de tiempo en que los sistemas han permanecido inutilizados y/o el necesario para restaurar su funcionamiento, factores íntimamente ligados a la pérdida de capacidad de actuación o al lucro cesante sufrido por la imposibilidad de uso de los datos o sistemas durante ese tiempo, las consecuencias que podrían derivarse a efectos reputacionales para la empresa, entidad o persona física el haber sido víctima de un ataque informático, y, finalmente, los perjuicios para el directamente ofendido y para el interés general, los bienes jurídicos afectados por la acción ilícita, o el riesgo que se generar para intereses públicos o privados por la pérdida de los datos, programas o documentos. Y GIL GIL, 2021, p.469, alude a que la lesión a la ciberseguridad (este es el bien jurídico protegido) produce efectos directos, pues afecta al funcionamiento de la empresa o de la organización, generando como coste directo el reemplazo del sistema de seguridad, y costes indirectos, derivados de la pérdida de la actividad, de reputación, la fiabilidad y credibilidad de la organización. Más adelante recurre a los parámetros fijados en la Circular FGE 3/2017 (pp. 482 s.).

[48] Tales dudas surgen si tenemos en cuenta la ubicación sistemática, la estructura y el tenor literal de los preceptos reguladores de la responsabilidad penal de las personas jurídicas, por un lado, y de los delitos imprudentes, por otro lado. Por ejemplo, en el Capítulo dedicado a los delitos contra la salud pública desde los arts. 359 a 365 se tipifican los diferentes delitos dolosos, en el art. 366 se establece que, cuando de acuerdo con lo establecido en el art. 31 bis una persona jurídica sea responsable de los *delitos recogidos en los artículos anteriores* de este Capítulo, y el art. 367 dispone que si *los hechos previstos en todos los artículos anteriores* fueran realizados por imprudencia grave. O en el capítulo dedicado a delitos contra los recursos naturales y el medio ambiente, la estructura es como sigue: los arts. 325 a 327 se tipifican los primeros delitos dolosos, en el art. 328 se dispone que, cuando de acuerdo con lo establecido en el art. 31 bis una persona jurídica sea responsable *de los delitos recogidos en este Capítulo*; en los arts. 329 y 330 se tipifican otros delitos dolosos (el primero es el de prevaricación ambiental, el segundo el de daños en un espacio natural protegido); y en el art. 331 se establece que *los hechos previstos en este Capítulo* serán sancionados, en su caso, con la pena inferior en grado, en sus respectivos supuestos, cuando se hayan cometido por imprudencia grave.

o especial respecto de los restantes delitos de daños. Y a ello contribuyen, en su caso, las siguientes consideraciones.

Hay que comenzar indicando que la actual regulación de los arts. 264 a 264 quater CP es el resultado de la ratificación del Convenio del Consejo de Europa sobre la ciberdelincuencia, firmado en Budapest el 23 de noviembre de 2001, por un lado, y de la transposición al Derecho interno de la Decisión Marco 2005/222/JAI en un primer momento (en la reforma de 2010) y posteriormente de la Directiva 2013/40/UE (en la reforma de 2015).

En estos textos normativos se reclama la tipificación penal de los delitos de interferencia en los datos o en los sistemas informáticos, cuando las conductas de interferencia se cometan de manera deliberada (Convenio) o la interferencia ilegal en datos o los sistemas informáticos, cuando las conductas de interferencia se cometan de manera intencionada (Directiva). Es decir, en ninguno de los textos normativos se reclama la tipificación de delitos de daños informáticos (en la terminología del CP) cometidos de manera imprudente. Es más, literalmente se está proponiendo la tipificación recurriendo a especiales elementos subjetivos del injusto (deliberadamente, intencionadamente), lo que, de haberse trasladado a la redacción de los arts. 264 y 264 bis hubiera generado la duda incluso de si serían punibles los daños informáticos cometidos con dolo eventual[49].

Si el Convenio de Budapest y la Directiva 2013/40/UE obligan al Estado español a tipificar los delitos de daños informáticos dolosos, con el objetivo además de unificar la tipificación penal de determinados ciberdelitos que faciliten la cooperación internacional para su prevención y persecución, porque será habitual que esté presente su carácter transnacional, de esto habría que deducir que la voluntad del legislador español de 2010, primero, y el de 2015 después, era y es solo la tipificación de delitos de daños informáticos dolosos, sin tomar realmente conciencia de lo que podía o puede generar su ubicación concreta y el lugar exacto que ocupan dentro del Capítulo dedicado a los daños. De hecho, si se comprueban los Preámbulos de la LO 5/2010 y de la LO 1/2015, en la justificación de la reforma del antiguo art. 264.2 primero y del art. 264 después se comprueba que la intención del legislador no era otra que la transposición de la normativa europea al Derecho interno[50]. Y si, pese a

[49] Los delitos con especiales elementos subjetivos del injusto, exigiendo la actuación con una determinada intención o propósito, plantean la duda de si permiten o no su comisión con dolo eventual. Sobre ello véase, por todos, LUZÓN PEÑA, 2016, p. 164; MARTÍNEZ-BUJÁN PÉREZ, 2021, pp. 863 y ss.

[50] Así, en el Punto XIV del Preámbulo de la LO 5/2010 se afirmaba lo siguiente: "En el marco de los denominados delitos informáticos, para cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos". Y en el Punto I del Preámbulo de la LO 1/2015, dentro de la justificación general de la reforma, se afirma que "buena parte de las modificaciones llevadas a cabo están justificadas por la necesidad de atender compromisos internacionales. Así la reforma se ocupa de la transposición …. de la Directiva 2013/40/UE". Y más adelante, en el punto XIII, centrando la explicación de los cambios operados en los delitos informáticos, se afirma que la reforma lleva a cabo la transposición de la Directiva 2013/40/UE, añadiendo que las modificaciones propuestas pretenden superar las

todo, se sigue dando importancia decisiva a la ubicación sistemática, entonces la operatividad de la tipificación penal de los daños informáticos imprudentes se verá muy limitada si para su persecución penal se tiene que recurrir a la cooperación internacional, pues en este caso entraría en juego el principio de doble incriminación (los daños informáticos imprudentes no están tipificados en otros ordenamientos jurídicos).

Desde un plano teórico se reconoce la existencia de ciberdelitos, categoría que abarca a una serie de figuras delictivas, en mayor o menor número dependiendo de si utiliza aquel término en sentido estricto o amplio. El propio Convenio de Budapest reclama la tipificación de una serie de delitos que se agrupan de la siguiente manera: en el Título I los delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos (serían los delitos tipificados en los arts. 197 bis y 264-264 quater); en el Título II los delitos informáticos, donde se incluyen los de falsificación informática (que se corresponderían con los delitos de falsedad documental) y de fraude informático (que se correspondería con el delito de estafa informática); y en el Título III delitos relacionados con el contenido, donde se incluyen los delitos de pornografía infantil y los delitos relativos a la propiedad intelectual y derechos afines.

En sentido amplio (y es el concepto utilizado en el Convenio de Budapest) se pueden llegar a catalogar como ciberdelitos, así denominados porque las TIC`s son los medios comisivos, delitos contra la intimidad y la propia imagen, la libertad e indemnidad sexual, el estado civil, delitos contra el patrimonio, delitos relativos a la propiedad intelectual e industrial, el mercado y los consumidores, delitos contra el orden socioeconómico, delitos contra la fe pública, delitos contra el orden público, delitos contra la paz pública, delitos contra la seguridad del Estado[51]. Pues bien, en esta amplia enumeración de modalidades delictivas, abstrayendo el componente cibernético (sea este utilizado o no en la tipificación penal de las diferentes modalidades delictivas abarcadas por tales expresiones), resulta muy excepcional la tipificación de delitos imprudentes, solo hay algún delito imprudente en el caso de delitos contra el patrimonio y el orden socioeconómico (daños, blanqueo de capitales) y en delitos contra la fe pública (en falsedad de documentos públicos u oficiales cometida por autoridad o funcionario público), así que tiene que resultar también muy excepcional la incriminación imprudente cuando estos delitos se cometan a través de medios relacionados con la informática y/o las TIC`s, exigiendo en todo caso una tipificación expresa de la modalidad imprudente para que no haya ninguna duda sobre la decisión del legislador en este sentido. No tendría entonces suficiente peso argu-

limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea.

[51] Es la enumeración que realizan CÁMARA/CANO/GARCÍA/GIL (coord.)/HERNÁNDEZ (coord.)/MARTÍN/PASTOR/ROBLES/TOBARRA, 2019, pp. 162 y ss.

mentativo entender que con el art. 267 CP se estaría cumpliendo la exigencia de tipificación expresa de la modalidad imprudente de los daños informáticos: se trata del precepto dedicado genéricamente a los daños imprudentes, no se alude específicamente a los daños informáticos imprudentes.

En los ciberdelitos en sentido amplio no se está ante la protección de nuevos bienes jurídicos, sino ante formas de ataque nuevas y/o más graves. Solo en los denominados ciberdelitos puros o en sentido estricto, esto es, aquellos en los que las TIC`s son el objeto y el medio de ataque, se plantea la posible aparición de un nuevo bien jurídico, se configure como la seguridad informática, la confianza en el funcionamiento de los sistemas informáticos, o más específicamente, como la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. En el hipotético caso de que se admitiera la aparición de este nuevo bien jurídico, y que se justificara además la intervención penal para su protección y salvaguarda (pasa a ser un bien jurídico-penalmente relevante), parece más ajustado a los límites de la potestad punitiva del Estado que tal protección se establezca frente a conductas dolosas que lo lesionen o lo pongan en peligro, descartando la punibilidad de las conductas imprudentes[52]. Y si además este bien jurídico es de carácter supraindividual o colectivo, con más motivo se ha de reclamar la limitación de la tipificación penal a las conductas dolosas que lo lesionen/pongan en peligro, pues así también se ha decidido respecto de otros delitos que protegen bienes jurídicos colectivos, con excepciones puntuales referidas sobre todo a los delitos contra la seguridad colectiva y delitos contra el medio ambiente, es decir, las excepciones, incriminando delitos imprudentes, se han planteado respecto de delitos que protegen bienes jurídicos supraindividuales o colectivos que sirven o están orientados a la protección de bienes jurídicos individuales como la vida, integridad y salud[53]. Así se ha decidido en la normativa del Consejo de Europa y de la UE antes mencionada al reclamar la tipificación dolosa de los delitos de acceso ilegal a sistemas informáticos y de interferencia en datos y sistemas informáticos.

Por último, algunas de las conductas constitutivas de daños informáticos, que dan lugar ya a las cualificaciones de primer nivel, presentan grandes similitudes con el

[52] ROMEO CASABONA, 1996, pp. 414 s., 440 y ss., ha planteado las dos formas posibles de proceder en la tipificación de delitos informáticos (ahora de ciberdelitos), una, a través de la introducción de tipos de equivalencia (tipos equivalentes a los delitos "tradicionales" donde ya se ha definido de manera más o menos clara el bien jurídico protegido), la otra, a través de la introducción de nuevas figuras delictivas que han de proteger un nuevo bien jurídico, que ha de ser definido con carácter previo entonces. Este autor se decanta por la primera de las técnicas pero no descarta la hipótesis de que se tenga que crear algún tipo penal nuevo que tenga por objeto de protección un nuevo bien jurídico. Pero en este caso propone que la incriminación se limite a las conductas intencionales, para evitar el castigo no deseado de conductas negligentes o de errores o fallos técnicos.

[53] Claramente en los delitos contra la seguridad colectiva se ve la orientación a la protección de la vida, la integridad, la salud de las personas, porque además en su descripción típica se hace esta referencia, si no en todos los delitos, en la mayoría de ellos. Y lo mismo ha de entenderse en el caso de los delitos contra los recursos naturales y el medio ambiente, aunque se admita la concepción ecocéntrica del bien jurídico medio ambiente. Sobre esto último v., por todos, MARTÍNEZ-BUJÁN PÉREZ, 2019, pp. 995 s.

delito de desórdenes públicos del art. 560 CP[54]. En este precepto se castiga a quien cause daños que interrumpan, destruyan, obstaculicen líneas o instalaciones de telecomunicaciones o la correspondencia postal, cause daños en las vías férreas o que originen un grave daño en la circulación ferroviaria, o dañe las conducciones o transmisiones de agua, gas, electricidad para las poblaciones, interrumpiendo o alterando gravemente el suministro o servicio. Por cierto, como ya se ha indicado anteriormente, en este precepto el verbo dañar amplía su significado, abarcando como resultados no solo la destrucción o deterioro de la cosa, sino la interrupción, la obstaculización, la alteración, resultados que también aparecen mencionados en los arts. 264 y 264 bis. En el delito de desórdenes públicos, que solo puede cometerse dolosamente, se pretende garantizar los servicios esenciales de telecomunicaciones, correspondencia postal, transporte ferroviario, gas, agua, electricidad; en los arts. 264 y 264 bis se ha previsto como circunstancias cualificantes que el hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad (arts. 264.2.3ª y 264 bis.2), y que los hechos hayan afectado al sistema informático de una infraestructura crítica (arts. 264.2.4ª y 264 bis.2). Dada la similitud con este delito, si el de desórdenes públicos solo admite su comisión dolosa, también se podría llegar a la conclusión de que los delitos daños informáticos cualificados de primer nivel tendrían que ser cometidos dolosamente. Y si tal conclusión se hace respecto de los delitos cualificados de primer nivel, entonces la misma conclusión se tendría que hacer extensiva al resto de delitos cualificados (de primer nivel cuando concurran las otras circunstancias cualificantes y de segundo y tercer nivel) y con más motivo respecto de los tipos básicos de daños informáticos.

[54] Ya con la anterior regulación de los daños informáticos, MARCHENA GÓMEZ, 2001, pp. 363 s., advertía de que su planteamiento como una modalidad agravada del delito de daños no abarcaba la verdadera ofensividad de los hechos que están detrás de las conductas que se subsumían (y se subsumen) en aquel delito, poniendo como ejemplo la destrucción generalizada de programas de gestión del correo electrónico, un hecho que podría ser subsumido en el delito de desórdenes públicos del art. 560 (si el correo electrónico encaja en el tenor literal de correspondencia postal). Con más claridad, GONZÁLEZ HURTADO, 2014, pp. 1 y ss., 5 y ss.; 2016, pp. 60 y ss., 70, en su tesis a favor de la protección de un nuevo bien jurídico, la seguridad de los sistemas informáticos, afirma que su protección frente a la lesión o puesta en peligro se llevaría a cabo a través de los delitos de acceso ilícito, intrusismo informático, daño y sabotaje informático, abuso de dispositivos y desórdenes públicos en las telecomunicaciones. Y añade que los delitos destinados a proteger este nuevo bien jurídico deberían ser reubicados dentro de los delitos contra el orden público, en concreto, como delitos de desórdenes públicos, o, en su caso, planteándose como hipótesis la posibilidad de una regulación diferenciada, entre delitos informáticos que atentan contra el orden público y los delitos informáticos que vulneran otro bien jurídico. Concluye su argumentación destacando las similitudes existentes entre los delitos de daños informáticos de los arts. 264 y 264 bis y el de desórdenes públicos del art. 560 (si bien reconoce que no todos los casos de daños informáticos tienen la misma gravedad, tal como se percibe de la propia regulación diferenciando entre tipos básicos y tipos cualificados, de primer, segundo y tercer nivel). Con la actual regulación, RODRÍGUEZ MESA, 2017, p. 83, recurre a las reglas del concurso de delitos entre las modalidades agravadas del art. 264.2 circunstancias 3ª y4ª y el delito de desórdenes públicos del art. 560, para el caso de que efectivamente se cumplan los elementos típicos de esta modalidad delictiva, algo que sí resulta difícil. Esta autora plantea tal solución concursal para poder abarcar todo el desvalor del hecho resultante en casos como estos, pues en los tipos penales de daños informáticos se protege el bien jurídico seguridad de la información, claramente diferente al protegido en el delito de desórdenes públicos.

Ciertamente, este argumento es bastante endeble, ya que se podría refutar alegando que, en el delito de desórdenes públicos, de manera indubitada, el legislador ha decidido tipificar solo la comisión dolosa, pero ha utilizado otro criterio en la tipificación de los daños informáticos, por la previsión "genérica" del art. 267 CP. Pero en este caso, para los supuestos en los que sí se percibe la similitud entre desórdenes públicos/daños informáticos[55], habría que encontrar la razón por la que el legislador ha tipificado solo el delito doloso en los desórdenes públicos y, sin embargo, ha "querido" tipificar delitos dolosos e imprudente de daños informáticos que afectan a servicios públicos esenciales.

IV. **Recapitulación**

Como ha quedado demostrado a lo largo de este comentario, se pueden encontrar argumentos a favor y en contra de la punibilidad de los daños informáticos imprudentes. El principal argumento a favor de la punibilidad de los daños informáticos imprudentes se desprende de la ubicación sistemática, con la trascendencia que de ello se deriva. Los argumentos en contra de la punibilidad de los daños informáticos imprudentes son de diversa índole, como se ha tratado de explicar a lo largo de estas páginas, conectando algunos de ellos con una cuestión previa, abierta también a la discusión, sobre el objeto de protección de estos ciberdelitos. Políticocriminalmente parece más

[55] Si, efectivamente, se percibe la similitud entre los desórdenes públicos y los daños informáticos cuando el hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o hayan afectado al sistema de una infraestructura crítica (arts. 264.2 y 264 bis.2), en tal caso será necesario establecer las diferencias entre ambas modalidades delictivas, condición previa para la posterior solución del eventual concurso (de leyes o delitos) entre ambas infracciones penales. La primera de las diferencias ha de fijarse en la diferente ubicación sistemática, lo que puede ser indicativo (no es concluyente) del objeto de protección en cada uno de ellos: los arts. 264 a 264 quater están ubicados en el Título dedicado a delitos contra el patrimonio y el orden socioeconómico, en el Capítulo dedicado a los daños, el art. 560 está ubicado en el Título dedicado a los delitos contra el orden público, en el Capítulo sobre los desórdenes públicos. La segunda y más trascendental diferencia se refiere al objeto material sobre el que recae la conducta típica: en el art. 264 son los datos informáticos, programas informáticos, documentos electrónicos; en el art. 264 bis son los sistemas informáticos; en el art. 560 son las líneas o instalaciones de telecomunicaciones o la correspondencia postal, las vías férreas, elementos que intervienen en el desarrollo de la circulación ferroviaria, las conducciones o transmisiones de agua, gas, electricidad. Conectado con esto, hay una diferencia más, la gravedad del daño, un elemento exigido en los daños informáticos, no lo es en los desórdenes públicos, salvo alguna excepción (sí se exige que haya grave daño para la circulación ferroviaria o interrupción o alteración grave en el suministro o servicio de agua, gas, electricidad). Es más, en los daños informáticos se exige una doble referencia sobre la gravedad, una, para fijar la concurrencia de la conducta típica-resultado (en el art. 264.1 de manera grave borre, dañe, deteriore, altere, suprima, haga inaccesible, cuando el resultado sea grave; en el art. 264 bis.1 de manera grave obstaculice o interrumpa), y otra, para la concurrencia de la circunstancia cualificante: perjudique gravemente el funcionamiento de servicios públicos esenciales (y habría una tercera referencia a la gravedad en la cualificación de segundo nivel, si los hechos hubieran resultado de extrema gravedad). No hay auténtica diferencia, es mera apariencia, en las conductas típicas: en el art. 560 es causar daños, pero esta conducta ha de provocar como resultados la interrupción, la obstaculización, la destrucción, daño para la circulación ferroviaria, la alteración; en el art. 264 se describen diferentes conductas-resultados consistentes en borrado, daño, deterioro, alteración, supresión, hacer inaccesible; más claramente, en el art. 264 bis.1 los resultados son obstaculización, interrupción.

razonable la opción a favor de la no punibilidad de los daños informáticos imprudentes.

En aras de la seguridad jurídica es precisa la aclaración de esta cuestión. Mientras tanto, ciertamente, no parece que vaya a resultar muy frecuente que los tribunales tengan que resolver esta duda interpretativa, por dos motivos: el primero, porque la cuantía económica exigida en el art. 267 CP es lo suficientemente elevada, también desde la perspectiva de los daños informáticos, hasta el punto de que se puede aventurar que la misma se alcanzará solamente cuando se trate de daños causados a medianas y grandes empresas y a Administraciones Públicas. El segundo, porque para la persecución penal por el delito imprudente es necesaria la denuncia de la persona agraviada o de su representante legal. Y en el caso de empresas y Administraciones públicas primará el interés por mantener su "estatus" reputacional.

Bibliografía

ABADÍAS SELMA, A. (2021), *Derecho penal. Parte especial. Temas prácticos para su estudio,* Madrid.

AGUDO FERNÁNDEZ, E.; JAÉN VALLEJO, M.; PERRINO PÉREZ. A.L. (2018), *Derecho penal aplicado. Parte especial. Delitos contra el patrimonio y contra el orden socioeconómico,* Madrid.

ALMENAR PINEDA, F. (2018), *Ciberdelincuencia,* Porto.

ÁLVAREZ VIZCAYA, M (2001), "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red", *Cuadernos de Derecho Judicial,* n. X, pp. 255-280.

ANDRÉS DOMÍNGUEZ, A.C. (1999a), "Los daños informáticos en la Unión Europea", *La Ley,* n. 1, pp. 1724-1730.

ANDRÉS DOMÍNGUEZ, A.C. (1999b), *El delito de daños: consideraciones jurídico-políticas y dogmáticas,* Burgos.

ANDRÉS DOMÍNGUEZ, A.C. (2009), "Los daños informáticos en el Derecho Penal europeo", en Álvarez García (dir.)/Álvarez García/Manjón-Cabeza Olmeda/Ventura Püschel (coords.): *La adecuación del Derecho penal español al ordenamiento de la Unión Europea. La política criminal europea*, Valencia, pp. 411-426.

ANDRÉS DOMÍNGUEZ, A.C. (2010), "Daños (arts. 263, 264, 267 y 626)", en Álvarez García/González Cussac (dirs.): *Comentarios a la reforma penal de 2010,* Valencia, pp. 291-296.

ANDRÉS DOMÍNGUEZ, A.C. (2011), "De los daños", en Álvarez García (dir.)/Manjón-Cabeza Olmeda/Ventura Püschel (coords.): *Derecho penal español. Parte especial,* vol. II, 1.ª edición, Valencia, pp. 417-433.

ANDRÉS DOMÍNGUEZ, A.C. (2015a), "Reformas en daños", en Quintero Olivares (dir.): *Comentario a la reforma penal de 2015,* Cizur Menor (Navarra), pp. 539-552.

ANDRÉS DOMÍNGUEZ, A.C. (2015b), "Artículos 264 a 264 quater", en Gómez Tomillo (dir.): *Comentarios prácticos al Código Penal,* vol. III, Cizur Menor (Navarra), pp. 347-363.

BALEA ROUCO, A. (2021), "Copias de seguridad, delitos de daños informáticos y grado de ejecución", *La Ley,* n. 9939, pp. 1-8.

BARDAVÍO ANTÓN, C. (2020), "Ciberdelitos: evolución hacia un Derecho penal funcional incorrectamente dogmatizado", en Bustos Rubio/Abadías Selma (dirs.): *Una década de reformas penales. Análisis de diez años de cambios en el Código Penal (2010-2020),* Barcelona, pp. 393-414.

BARRIO ANDRÉS, M. (2012), "El régimen jurídico de los delitos cometidos en internet en el derecho español tras la reforma penal de 2010", en: *Delincuencia informática: tiempos de cautela y amparo*, Cizur Menor (Navarra), pp. 31-56.

BARRIO ANDRÉS, M. (2016), "Hacking, cracking, grooming y otras conductas ilícitas en internet en el Código Penal español", *La Ley Penal,* n. 121, pp. 1-24.

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

BENÍTEZ ORTÚZAR, I.F. (2020), "Delitos contra el patrimonio y el orden socioeconómico", en Morillas Cueva (dir.): *Sistema de Derecho penal. Parte especial,* 3.ª edición, Madrid, pp. 647-678.

CÁMARA ARROYO, S.; CANO CARRILLO, J.; GARCÍA RUIZ, A.; GIL GIL, A. (coord.); HERNÁNDEZ BERLINCHES, R. (coord.); MARTÍN FERNÁNDEZ, C.; PASTOR VARGAS, R.; ROBLES GÓMEZ, A.; TOBARRA ABAD, LL. (2019), *Cibercriminalidad,* Madrid.

CARRASCO ANDRINO, M.M. (2009), "El acceso ilícito a un sistema informático", en Álvarez García (dir.)/Álvarez García/Manjón-Cabeza Olmeda/Ventura Püschel (coords.): *La adecuación del Derecho penal español al ordenamiento de la Unión Europea. La política criminal europea*, Valencia, pp. 341-364.

CORCOY BIDASOLO, M. (1990) "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", *La Ley,* n. 1, pp. 1000-1016 [= en Mir Puig (coord.), *Delincuencia informática*, Barcelona, 1992, pp. 177-182].

CORCOY BIDASOLO, M. (2007), "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", *Eguzkilore,* n. 21, pp. 7-32.

CORCOY BIDASOLO, M. (2015), "Artículos 264 a 264 quater", en Corcoy Bidasolo/Mir Puig (dirs.)/Vera Sánchez (coord.): *Comentarios al Código Penal. Reforma LO 1/2015 y LO 2/2015,* Valencia, pp. 931-938.

CORCOY BIDASOLO, M. (2019), "Daños. Sabotaje informático (arts. 263-267)", en Corcoy Bidasolo (dir.)/Hortal Ibarra (coord.): *Manual de Derecho penal. Parte especial* vol. I, 2.ª edición, Valencia, pp. 572-.583.

CRUZ DE PABLO, J. A. (2006), *Derecho penal y nuevas tecnologías. Aspectos sustantivos*, Madrid.

DAVARA FERNÁNDEZ DE MARCOS, E.; DAVARA FERNÁNDEZ DE MARCOS, L.; DAVARA RODRÍGUEZ, M.Á. (coord.) (2017), *Delitos informáticos,* Cizur Menor (Navarra).

DE LA MATA BARRANCO, N.J. (2007), "Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general", *Cuadernos Penales José María Lidón*, n. 4, pp. 41-84.

DE LA MATA BARRANCO, N.J. (2010), "El delito de daños a datos, programas, documentos y sistemas informáticos", en Juanes Peces (dir.): *Reforma del Código Penal. Perspectiva económica tras la entrada en vigor de la LO 5/2010, de 22 de junio. Situación jurídico-penal del empresario,* Madrid*,* pp. 149-178.

DE LA MATA BARRANCO, N.J. (2016a), "Los delitos contra la integridad y disponibilidad de datos y sistemas informáticos después de la LO 1/2015", en Badigalupo Saggese/Feijoo Sánchez/Echano Basaldua (coords.), *Estudios de Derecho penal. Homenaje al profesor Miguel Bajo,* Madrid, pp. 1089-1108.

DE LA MATA BARRANCO, N.J. (2016b), "Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito (art. 197 bis CP). El concepto de privacidad informática y la tutela del buen funcionamiento de los sistemas de información y comunicación", *Cuadernos de Política Criminal,* n. 118, pp. 43-86.

DE LA MATA BARRANCO, N.J. (2018), "Delitos contra los sistemas de información", en de la Mata Barranco/Dopico Gómez-Aller/Lascurain Sánchez/Nieto Martín: *Derecho penal económico y de la empresa*, Madrid, pp. 727-759.

DE LA MATA BARRANCO, N.J.; HERNÁNDEZ DÍAZ, L. (2009), "El delito de daños informáticos: una tipificación defectuosa", *Estudios Penales y Criminológicos,* n. XXIX pp. 311-362.

DE LA MATA BARRANCO, N.J.; HERNÁNDEZ DÍAZ, L., (2010a), "Los delitos vinculados a la informática en el Derecho penal español", en de la Cuesta Arzamendi (dir.)/de la Mata Barranco (coord.): *Derecho penal informático,* Cizur Menor (Navarra), pp. 159-200.

DE LA MATA BARRANCO, N.J.; HERNÁNDEZ DÍAZ, L. (2010b), Un ejemplo de delitos informáticos: delitos contra sistemas y datos en el Código Penal español: ¿delitos de daños?", en de la Cuesta Arzamendi (dir.)/de la Mata Barranco (coord.): *Derecho penal informático,* Cizur Menor (Navarra), pp. 201-246.

DE LA MATA BARRANCO, N.J.; HERNÁNDEZ DÍAZ, L. (2011), "El Derecho penal frente a las nuevas realidades criminales: el ejemplo del denominado sabotaje informático", en Hormazábal Malarée (coord.): *Estudios de Derecho penal en memoria del profesor Juan José Bustos Ramírez*, México, pp. 631-658.

DE URBANO CASTRILLO, E. (2007), "Artículos 263 a 267", en Conde-Pumpido Tourón (dir.)/López Barja de Quiroga (coord.): *Comentarios del Código Penal,* vol. III. Artículos 205 al 318, Barcelona, pp. 2115-2134.

DE URBANO CASTRILLO, E. (2012), "Los delitos informáticos tras la reforma del Código Penal de 2010", en: *Delincuencia informática. Tiempos de cautela y amparo,* Cizur Menor (Navarra), pp. 17-30.

ECIJA (2019), *Memento práctico Derecho de las Nuevas Tecnologías*, Madrid.

ESTRADA CUADRAS, A. (2016), "Daños informáticos y ataques de denegación de servicios", en Ayala Gómez/Ortiz de Urbina Gimeno (coords.): *Memento práctico penal económico y de la empresa,* Madrid, nm. 4620-4735 (pp. 519-533).

FERNÁNDEZ DÍAZ, C.R. (2018), "El delito de daños y el espionaje empresarial: dos ataques compatibles contra la información como bien inmaterial", *Indret,* n. 1, pp. 1-28.

FERNÁNDEZ PALMA, R.; MORALES GARCÍA, Ó. (2000), "El delito de daños informáticos y el caso *Hispahack", La Ley,* n. 1, pp. 1522-1529.

FERNÁNDEZ TERUELO, J. G. (2007), *Cibercrimen. Los delitos cometidos a través de internet -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la red-*, Oviedo.

FERNÁNDEZ TERUELO, J. G. (2010), "Daños informáticos: art. 264.1 CP", en Álvarez García/González Cussac (dirs.)/Manjón-Cabeza Olmeda/Ventura Püschel (coords.): *Consideraciones a propósito del Proyecto de Ley de 2009 de modificación del Código Penal*, Valencia, pp. 249-251.

FERNÁNDEZ TERUELO, J. G. (2011), *Derecho penal e internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, Valladolid.
GARCÍA ARÁN, M. (2004), "Artículos 263 a 267", en Córdoba Roda/García Arán (dirs.): *Comentarios al Código Penal. Parte especial*, vol. I, Madrid, pp. 918-942.
GARCÍA GONZÁLEZ, J. (2005), "Artículos 263 y 264", en Cobo del Rosal (dir.): *Comentarios al Código Penal,* vol. VIII, Madrid, pp. 739-782.
GIL GIL, A. (2021), "Daños informáticos", en: Sanz Delgado/Fernández Bermejo (coords.), *Tratado de delincuencia cibernática,* Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2021, pp. 467-510.
GONZÁLEZ CAMPO, E. (2018), "Los daños. Sabotaje informático", en Zárate Conde (coord.): *Derecho penal. Parte especial,* 2.ª edición, Madrid, pp. 425-437.
GONZÁLEZ HURTADO, J. A. (2014), "Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: la seguridad en los sistemas de información", *La Ley Penal,* n. 107, pp. 1-21.
GONZÁLEZ HURTADO, J. A. (2016), "La seguridad en los sistemas de información como un bien jurídico de carácter autónomo. Perspectiva europea y española", *Revista Penal México,* n. 9, pp. 59-76.
GONZÁLEZ RUS, J. J. (1999), "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", *Revista Electrónica de Ciencia Penal y Criminología,* n. 01-14.
GONZÁLEZ RUS, (2002), "Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (artículo 264.2 del Código Penal)", en Díez Ripollés/Romeo Casabona/Gracia Martín/Higuera Guimerá (eds.): *La ciencia del Derecho penal ante el nuevo siglo. Libro homenaje al profesor doctor Don José Cerezo Mir,* Madrid, pp. 1281-1298.
GONZÁLEZ RUS, (2005a), "Artículo 264.2", en Cobo del Rosal (dir.): *Comentarios al Código Penal,* vol. VIII, Madrid, pp. 783-797.
GONZÁLEZ RUS (2005b), "Daños a través de internet y denegación de servicios", en: *Homenaje al profesor Dr. Gonzalo Rodríguez Mourullo,* Madrid, pp. 1469-1488.
GONZÁLEZ RUS, J. J. (2006), "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes", en Romeo Casabona (coord.): *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político criminales*, Granada, pp. 241-271.
GONZÁLEZ RUS, J.J. (2007), "Precisiones conceptuales y político-criminales sobre la intervención penal en internet", *Cuadernos Penales José María Lidón*, n. 4, pp. 13-40.
GORJÓN BARRANCO, M.C. (2021), "Sabotaje informático a infraestructuras críticas: análisis de la realidad criminal recogida en los artículos 264 y 264 bis del Código Penal. Especial referencia a su comisión con finalidad terrorista", *Revista de Derecho Penal y Criminología,* n. 25, pp. 77-124.
GUÉREZ TRICARICO, P. (2021), "Daños", en Molina Fernández (coord.): *Memento práctico penal,* Madrid, nm. 11650-11694/(pp. 1413-1421).
GUTIÉRREZ FRANCÉS, M.L. (1996), "Delincuencia económica e informática en el nuevo Código Penal", *Cuadernos de Derecho Judicial,* n. XI, pp. 247-306.
GUTIÉRREZ MAYO, E. (coord.); CASTRO ROMERO, V.; PÉREZ GOLPE, I. (2021), *Delitos informáticos. Paso a paso,* Madrid.
HERNÁNDEZ DÍAZ, L. (2009), "El delito informático", *Eguzkilore,* n. 23, pp. 227-247.
HERNÁNDEZ DÍAZ, L. (2010), "Aproximación a un concepto de Derecho penal informático", en de la Cuesta Arzamendi (dir.)/de la Mata Barranco (coord.): *Derecho Penal informático,* Cizur Menor (Navarra), pp. 31-54.

HERRERO-TEJEDOR ALGAR, F. (2011), "Delitos informáticos", en Agúndez/Martínez-Simancas Sánchez (dirs.)/Torres-Dulce Lifante (coord.): *Cuadernos de Derecho para ingenieros. La nueva reforma del Código Penal,* Madrid, pp. 137-156.

LIRA ARTEAGA, O.M. (2018), *Ciberdelitos. Perspectiva para su persecución,* Ciudad de México.

LÓPEZ MUÑOZ, J. (2020), *Cibercriminalidad e investigación tecnológica,* Madrid.

LUZÓN PEÑA, D.M. (2016), *Lecciones de Derecho penal. Parte general,* 3.ª edición, Valencia.

MADRIGAL MARTÍNEZ PEREDA, C.; LANZAROTE MARTÍNEZ, P. (2018), "Artículos 264-267", en del Moral García (dir.)/Escobar Jiménez (coord.): *Código penal. Comentarios y jurisprudencia,* vol. II. Artículos 234 a 616 quater, Granada, pp. 1590-1602.

MANZANARES SAMANIEGO, J.L. (2016), *Comentarios al Código Penal,* Madrid.

MARCHENA GÓMEZ, M. (2001), "El sabotaje informático: entre los delitos de daños y desórdenes públicos", *Cuadernos de Derecho Judicial,* n. X, pp. 353-366.

MARTÍNEZ-BUJÁN PÉREZ, C. (2019), *Derecho penal económico y de la empresa. Parte especial,* 6.ª edición, Valencia.

MARTÍNEZ-BUJÁN PÉREZ, C. (2021), "¿Existen expresiones reveladoras del dolo directo en el CP español? en Abel Souto/Brage Cendán/Guinarte Cabada/Martínez-Buján Pérez/Vázquez-Portomeñe Seijas (coords.): *Estudios penales en homenaje al profesor José Manuel Lorenzo Salgado,* Valencia, pp. 86-877.

MATA Y MARTÍN, R. (2001), *Delincuencia informática y Derecho penal,* Madrid.

MATA Y MARTÍN, R. (2021), "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 profesor José Manuel Lorenzo Salgado,* Valencia, pp. 893-914.

MATELLANES RODRÍGUEZ, N. (2000), "Algunas notas sobre las formas de delincuencia informática en el Código Penal", en Diego Díaz-Santos/Sánchez López (coords.): *Hacia un Derecho penal sin fronteras*, Madrid, pp. 129-150.

MAZUELOS COELLO, J. (2007), "Modelos de imputación en el Derecho penal informático", *Derecho Penal y Criminología* n. 28, pp. 37-54.

MESTRE DELGADO, E. (2021a), "Los daños", en Lamarca Pérez (coord.): *Delitos. La parte especial del Derecho Penal,* 6.ª edición, Madrid, pp. 443-451.

MESTRE DELGADO, E. (2021b), "Introducción", en: Sanz Delgado/Fernández Bermejo (coords.), *Tratado de delincuencia cibernática,* Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2021, pp. 31-71.

MIRÓ LLINARES, F. (2010), "Delitos informáticos: hacking. Daños", en Ortiz de Urbina Gimeno (coord.): *Reforma penal de 2010. Ley Orgánica 5/2010,* Madrid, nm. 1430-1520 (pp. 141-167).

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

MORALES GARCÍA, O. (2010), "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas, arts. 197.3 y 8, 264 y 248 CP, en Quintero Olivares (dir.): *La reforma penal de 2010. Análisis y comentarios,* Cizur Menor (Navarra), pp. 181-194.

MORALES GARCÍA, O. (2012), "Comentario los delitos informáticos de los arts. 197, 248 y 264 CP, en: *Delincuencia informática: tiempos de cautela y amparo,* Cizur Menor (Navarra), pp. 151-166.

MORALES PRATS, F. (2007), "Los delitos informáticos: dudas e incertidumbres en el Proyecto de reforma del Código Penal", *Cuadernos Penales José María Lidón*, n, 4, pp. 227-236.
MORENO ALCÁZAR, M.Á. (2020), "Daños", en Boix Reig (dir.): *Derecho penal. Parte especial*, vol. II, 2.ª edición, Madrid, pp. 375-391.
MORÓN LERMA, E. (2002), *Internet y Derecho penal: hacking y otras conductas ilícitas en la red*, 2.ª edición, Cizur Menor.
MORÓN LERMA, E. (2007), "Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos", *Cuadernos Penales José María Lidón,* n. 4, pp. 85-128.
MORÓN LERMA, E. (2010), "Daños informáticos: art. 264 CP", en Álvarez García/González Cussac (dirs.)/Manjón-Cabeza Olmeda/Ventura Püschel (coords.): *Consideraciones a propósito del Proyecto de Ley de 2009 de modificación del Código Penal*, Valencia, pp. 245-248.
MUÑOZ CONDE, F. (2021), *Derecho penal. Parte especial,* 23.ª edición, Valencia.
NIETO MARTÍN, A. (2019), "Delitos patrimoniales sin enriquecimiento: los daños", en Gómez Rivero (dir.): *Nociones fundamentales de Derecho penal. Parte especial*, vol. II, 3.ª edición, Madrid, pp. 2207-221.
ORTS BERENGUER, E. (2019), "Los daños", en González Cussac (coord.): *Derecho penal. Parte especial,* 6.ª edición, Valencia, pp. 499-505.
ORTS BERENGUER, E.; ROIG TORRES, M. (2001), *Delitos informáticos y delitos comunes cometidos a través de la informática*, Valencia.
PÉREZ BES. F. (coord.) (2021), *Memento práctico Ciberseguridad,* Madrid.
PICOTTI, L. (2006), "Internet y Derecho penal: ¿Un empujón únicamente tecnológico a la armonización internacional?, en Romeo Casabona (coord.): *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Granada, pp. 325-367.
QUERALT JIMÉNEZ, J.J. (2015), *Derecho penal español. Parte especial,* 7.ª edición, Valencia.
QUINTERO OLIVARES, G. (2001), "Internet y propiedad intelectual", *Cuadernos de Derecho Judicial,* n. X, pp. 367-398.
RAGUÉS I VALLÈS, R.; ROBLES PLANAS, R. (2012), "La reforma de los 'delitos informáticos': incriminación de los ataques a sistemas de información", en Silva Sánchez (dir.): *El nuevo Código Penal. Comentarios a la reforma*, Madrid, pp. 367-375.
RÍOS CORBACHO, J.M. (2016), "Delitos contra el patrimonio (IV). Daños", en Terradillos Basoco (coord.): *Derecho* penal. *Parte especial*, vol. I, 2.ª edición, Madrid, pp. 440-449.
ROBLES PLANAS, R.; PASTOR MUÑOZ, N. (2021), "Delitos contra el patrimonio (III)", en Silva Sánchez (dir.)/Ragués i Vallès (coord.): *Lecciones de Derecho penal. Parte especial,* 7.ª edición, Barcelona, pp. 287-313.
RODRÍGUEZ MESA, M.J. (2017), *Los delitos de daños. Capítulo IX del Título XIII del Código Penal tras la reforma de la LO 1/2015,* Valencia.
RODRÍGUEZ MOURULLO, G.; ALONSO GALLO, J.; LASCURAÍN SÁNCHEZ, J.A. (2001), "Derecho penal e internet", en Cremades García/Fernández-Ordóñez/Illescas Ortiz (coords.): *Régimen jurídico de internet*, Madrid, pp. 257-310.
ROMEO CASABONA, C.M. (1996), "Delitos informáticos de carácter patrimonial", *Revista Iberoamericana de Derecho Informático,* n. 9-11, pp. 413-442.
ROMEO CASABONA, C.M. (2006), "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,* Granada, 1-43.

ROMEO CASABONA, C.M. (2007), "De los delitos informáticos al cibercrimen", en: Pérez Álvarez/Núñez Paz/García Alfaraz (coords.), *Universitas vitae: homenaje a Ruperto Núñez Barbero,* Salamanca, pp. 649-670.

ROMEO CASABONA, C.M. (2012), "La penetración del Derecho penal económico en el marco jurídico europeo: los delitos contra los sistemas de información", en Romeo Casabona/Flores Mendoza (eds.): *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica*, Granada, 2012, pp. 331-373 [= en Fernández Teruelo (dir.)/González Tascón/Villa Sieiro (coords.), *Estudios penales en homenaje al profesor Rodrigo Fabio Suárez Montes*, Oviedo, 2013, pp. 611-656].

RUEDA MARTÍN, M.Á (2021), "La confidencialidad, integridad y disponibilidad de los sistemas de información y de comunicación como bien jurídico protegido en el Derecho penal", en Abel Souto/Brage Cendán/Guinarte Cabada/Martínez-Buján Pérez/Vázquez-Portomeñe Seijas (coords.): *Estudios penales en homenaje al profesor José Manuel Lorenzo Salgado,* Valencia, pp. 1309-1320.

SALVADORI, I. (2011), "Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010: perspectiva de Derecho comparado", *Anuario de Derecho Penal y Ciencias Penales,* pp. 221-252.

SERRANO TÁRRAGA, M.D. (2021), "Daños", en Serrano Gómez/Serrano Maíllo/Serrano Tárraga/Vázquez González, *Curso de Derecho penal. Parte especial,* 6.ª edición, Madrid, pp. 359-373.

VELASCO NÚÑEZ, E. (2019), en Velasco Núñez/Sanchís Crespo: *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015,* Valencia, pp. 21-251.

VIDAURRI ARÉCHIGA, M. (2019), "Delitos informáticos. Los retos del Derecho penal", en Nava Garcés (coord.): *Ciberdelitos,* Ciudad de México, pp. 197-220.

ZUGALDÍA ESPINAR, J.M. (2021), "Daños", en Marín de Espinosa Ceballos (dir.)/Esquinas Valverde (coord.): *Lecciones de Derecho penal. Parte especial*, 2.ª edición, Valencia, pp. 313- 316.