Estudios Penales y Criminológicos, vol. XXIX (2009). ISSN 1137-7550: 311-362

EL DELITO DE DAÑOS INFORMÁTICOS: UNA TIPIFICACIÓN DEFECTUOSA

Norberto J. de la Mata Barranco
Catedrático de Derecho Penal de la Universidad del País Vasco
Leyre Hernández Díaz
Investigadora del Gobierno Vasco en la Universidad del País Vasco

Resumen: El desarrollo de la informática y, especialmente, de Internet, en la sociedad actual, ha conllevado la proliferación de nuevas formas de ataque a derechos individuales o colectivos a las que el Derecho Penal se ha visto obligado a responder con cierto carácter de urgencia. El legislador penal español, en está necesidad de rápida adaptación a los nuevos tiempos, ha realizado algunas modificaciones en el articulado del Código Penal con una técnica no siempre adecuada. Uno de los nuevos preceptos incorporados en esta dinámica al texto punitivo que más críticas y desacuerdos doctrinales ha recibido es el artículo 264.2, referente a los daños en sistemas informáticos o en datos contenidos en los mismos. La propia creación del precepto, su ubicación sistemática, así como la redacción que ha recibido, suscitan dudas acerca de su naturaleza como tipo autónomo de daños o meramente agravado y, lo que es más importante, sobre el auténtico contenido de la conducta incriminada, que han abierto un debate sobre la posibilidad de considerar penalmente nuevos bienes jurídicos vinculados a la idea de la tutela de la libertad o seguridad informáticas.

Recibido: agosto 2009. Aceptado: octubre 2009

Palabras clave: Daños informáticos, Delincuencia informática, Delito de daños, Delito informático, Sabotaje informático, TICs y Derecho Penal.

Abstract: The development of computer technology and, especially, of the Internet, in modern society, has brought with it a proliferation of new forms of attack on individual or collective rights, obliging an urgent response from criminal law. Out of this necessity to quickly adapt to the new scenario, Spanish legislators have undertaken some modifications to the articles of the penal code, albeit with less than successful results. Of all the new articles introduced to the criminal code, the one which has raised the most criticism and debate is Art. 264.2, which refers to damage to computer systems or to information stored therein. The actual conception of the article, its position in the legal code and its wording, all raise doubts about whether it is an independent new crime or a speciality of damages; and more importantly, with respect to the true definition of the incriminated conduct. As a result, these questions have opened a debate over the possibility of how to incorporate these new and legally protected interests into the penal code, interests which are linked to the idea of safeguarding computer freedom or computer security.
Keywords: Computer Damage Crime, Computer Delinquency, Computer Crime, Computer Sabotage, Information and Communication Technologies and Criminal Law.

I. Los daños a los elementos lógicos de un sistema informático: cuestiones terminológicas

Antes de explicar en qué consisten los daños a los elementos lógicos de un sistema informático hay que diferenciar, en primer lugar, y aunque obviamente ya sea algo sabido, los términos *hardware* y *software*, ya que la respuesta del Derecho Penal frente al ataque a uno u otro tipo de componente informático puede ser diferente. El *hardware* refiere todos los componentes físicos del sistema informático. El *software*, sus componentes lógicos: aplicaciones, datos y programas que hacen funcionar o se ejecutan en el sistema informático. Un ataque a un sistema informático puede afectar a cualquiera de ambos; otra cuestión será de qué modo deba responder el Derecho Penal en uno u otro caso.

En cuanto al ataque a los componentes lógicos del sistema —al *software*—, éste puede realizarse de un modo básico, tradicional, físico, ajeno a lo que es la utilización de las TICs: por ejemplo, golpeando el ordenador, mojándolo, quemándolo, introduciendo cuchillas en la *CPU*[1]; pero también puede realizarse a través de medios comisitos novedosos, vinculados al desarrollo de las TICs: así, introduciendo virus, troyanos, gusanos, etc. En ambos casos podrá afectarse el funcionamiento del sistema y/o la disponibilidad de los datos contenidos en él.

En el caso de estas últimas modalidades comisivas, las mismas se han diversificado tanto que es necesario para entender de qué estamos hablando precisar algunos de los conceptos de la nueva terminología informática referida al modo en que puede producirse el posible ataque —y daño— informático.

Así, se habla de *software* malicioso o *malware* para describir un conjunto de códigos y programas, que, introducidos en un sistema informático, originan problemas de utilización u operatividad del mismo —de sus programas de funcionamiento— o alteración o borrado de datos.

Los *crash programs* o programas destructores hacen referencia a las rutinas (virus, gusanos, conejos, troyanos, etc.) encargadas de destruir gran cantidad de datos en un corto espacio de tiempo[2]. Los virus son códigos maliciosos creados para alterar un sistema informático que necesitan un programa anfitrión para reproducirse y transmitirse, al que se adhieren para su ejecución. Los gusanos (*Worms*) son piezas independientes de *software* que a diferencia de los virus son capaces de reproducirse a sí mismos y de auto transmitirse. Los conejos o bacterias son programas que, si bien en principio no dañan el sistema, se auto reproducen ocupando toda la memoria del sistema que, de esta forma, bloquean. Los troyanos son un *software* malicioso que, oculto en

---

1 Alude ya a esta posibilidad CORCOY BIDASOLO, "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", p. 1002.

2 Ampliamente, SIEBER, "Documentación para una aproximación al delito informático", p. 75.

un programa benigno o útil, se introduce en el sistema informático (incluso en teléfonos móviles o *PDAs*); una vez dentro del sistema, pueden generar un gran número de disturbios o daños en el mismo (borrado o daño en los datos o programas, utilizar el sistema para realizar ataques de denegación de servicios, robar datos y contraseñas, abrir puertas traseras para permitir a los atacantes controlar el sistema y convertir el ordenador en un zombi al servicio de éstos, etc.), lo que les convierte en especialmente peligrosos; los troyanos, en principio, no son capaces de reproducirse a sí mismos, pero, aun así, son en la actualidad la amenaza más importante, cuantitativamente hablando, en los ataques realizados a través de Internet, en detrimento de los virus tradicionales, que van perdiendo importancia[3].

Un nuevo tipo de troyano es el denominado *Backdoor* (puerta trasera) que permite a un atacante tomar el control remoto del sistema infectado para llevar a cabo una gran diversidad de acciones: espiar el escritorio remoto, realizar capturas de pantalla o de la *webcam*, subir o descargar archivos, alterar el funcionamiento normal del sistema, etc.

Es destacable también otro novedoso tipo de ataque que ha surgido en los últimos años, el de los denominados *blended threats*, especialmente peligrosos por combinar las características de virus, gusanos y troyanos con las vulnerabilidades de Internet y de sus servidores para crear, transmitir y propagar los ataques[4].

---

3 Según datos extraídos del Estudio sobre Seguridad de la Información y e-Confianza de los hogares españoles realizado por el Instituto Nacional de Tecnologías de la Comunicación (INTECO), publicado en junio de 2007 en su página www.inteco.es, las mayores amenazas a los sistemas informáticos, por su incidencia y gravedad, proceden en la actualidad de los troyanos (amenaza para el 50,3% de los equipos). La tradicional amenaza de los virus, en cambio, afecta al 10,1% de los ordenadores y sólo representa un 1,2% de las variantes de *malware* encontradas; esta pérdida de importancia se debe, por un lado, a la eficacia de los sistemas antivirus y de sus actualizaciones automáticas y, por otro, al abandono del desarrollo de virus en favor de troyanos y *adware*.

4 Véanse HUGHES/DE LONE, "Virus, Worms, and Trojan Horses. Serious Crimes, Nuisance or both?", p. 81.

El ataque se materializaría, por ejemplo, además de con el lanzamiento de un ataque *DoS*, con la instalación de un *backdoor* y con el daño de un sistema local. Las amenazas mixtas, además, pueden utilizar múltiples modos de transporte: así, el e-mail, *IRC* o archivos compartidos en redes *p2p*. Y el ataque no se limita a un solo acto, pudiendo modificar un ataque mixto, por ejemplo, archivos *.exe*, archivos *.html* y el registro al mismo tiempo.

Las bombas lógicas son rutinas introducidas en un programa para que al realizar una determinada acción, por ejemplo la copia del mismo, se produzcan alteraciones o daños en el programa. Las bombas de tiempo, como las lógicas, son rutinas introducidas en programas o archivos, pero para que se produzca una alteración del programa o daño al mismo en un momento determinado, al llegar una fecha concreta o pasar un plazo de tiempo establecido al efecto.

Los ataques de denegación de servicios (*DoS Attack* o *denial of service*) son conductas tendentes al bloqueo de un sistema informático mediante la saturación del mismo. Este bloqueo conlleva que los usuarios del sistema informático no puedan acceder a él o a ciertos recursos o datos del mismo durante el período de saturación, que a menudo se produce mediante un sistema de acumulación de peticiones de información que se rechazan automáticamente.

Son muchos otros los ataques que pueden producirse contra un ordenador —por ejemplo, últimamente prolifera el *adware* (*software* que muestra publicidad en ventanas emergentes, *banners*, etc., no solicitada), recopilando en ocasiones información sobre los hábitos de navegación de los usuarios para luego redirigirles a la publicidad coincidente con sus intereses—, pero que no tiene por qué afectar al correcto funcionamiento del sistema.

Como sinónimo de daño informático se utiliza el término "sabotaje informático" —*cyberpunking*, vandalismo informático, vandalismo electrónico, *cracking*[5] o, para algún autor o en

5 DE ALFONSO LASO, "El hackering blanco. Una conducta ¿punible o impune?", pp. 512 y ss., utiliza el término *cracker* para referirse al sujeto

Estudios Penales y Criminológicos, vol. XXIX (2009). ISSN 1137-7550: 311-362

alguna ocasión, también *hacking*[6]—, que hace referencia, en general, a todo el conjunto de conductas que dañan, impidiendo su correcto funcionamiento, elementos de naturaleza informática, quedando fuera del concepto, obviamente, conductas que se sirven del sistema para acceder a datos, redirigir conductas o introducir o distribuir información no deseada. Ahora bien, ni es necesaria la destrucción del objeto del ataque (en soporte o no), ni su desaparición total, ni un menoscabo funcional absoluto. Así, se ha descrito por algún autor el sabotaje como el conjunto de conductas de destrucción, inutilización o incapacitación de sistemas informáticos —englobando por supuesto en éstos los de carácter cibernético o telemático— o de datos o información contenida, transferida o transmitida en los mismos, así como de sus funciones de procesamiento y tratamiento, ya se lleven a cabo las mismas mediante utilización de métodos lógicos, informáticos o telemáticos, ya mediante el abuso de los equipos físicos que permiten el acceso a dichos sistemas o datos[7].

Pues bien, la definición de lo que se entiende por daño informático debe permitir incluir tanto la destrucción de sistemas informáticos completos como la de sus componentes concretos, ya sean equipos, datos, documentos o programas. Y, lo que conllevará no pocos problemas de tipificación, ha de abarcar tanto lo que es en sí la destrucción de tales elementos —o su inutilización— como

---

que se introduce en un sistema informático con el objetivo de realizar conductas de sabotaje informático; también, MATELLANES RODRÍGUEZ, "Vías para la tipificación del acceso ilegal a los sistemas informáticos", p. 51. GÓMEZ MARTÍN, "El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (art. 270, párr. 3º CP)", p. 3, o MORÓN LERMA, *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*, pp. 40 y ss., sin embargo, reservan este término para aquellas conductas que neutralizan sistemas de protección de un *software* con el fin de realizar copias no autorizadas del mismo.

6 Utilizan este término RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", p. 266, si bien el mismo se reserva por la mayoría de autores para conductas de intromisión en el sistema sin daño al mismo.

7 Descriptivamente, ROVIRA DEL CANTO, *Delincuencia informática y fraudes informáticos*, pp. 226 y ss.

la simple perturbación del funcionamiento del sistema completo o de alguno de sus componentes funcionales[8].

Dado que lo característico de los sistemas informáticos es su función de almacenamiento, procesamiento o transmisión de información, parece adecuado reservar el concepto de daño informático, al menos en este ámbito penal, para conductas que, de una u otra manera, afecten a los elementos lógicos del sistema; ya, sin embargo, mediante la destrucción de todo el sistema informático, ya mediante la de alguno de sus componentes: programas, datos o documentos[9], ya, a nuestro juicio, mediante la alteración de la funcionalidad del sistema por afectarse alguno de sus componentes físicos o lógicos que impiden un uso plenamente satisfactorio del mismo. Justamente teniendo en cuenta que la destrucción de elementos físicos, aunque no necesariamente, lo normal será que implique el daño de elementos lógicos, seguramente de imposible recuperación, aunque no se realice con ese propósito, el término ha de permitir incluir ataques tanto a elementos físicos como a elementos lógicos del sistema[10], en sus muy diversas modalidades, con independencia de dónde se ubiquen típicamente unos u otros.

Lo importante no es qué tipo de conducta se lleve a cabo, sino cuál sea su consecuencia; y si ésta es la de alteración, desaparición, destrucción, inutilización o menoscabo de componentes del sistema, que perjudiquen su funcionalidad (ya sea de sus aplicaciones, ya de sus programas, ya del acceso a sus datos), deberemos poder hablar de daño informático.

---

8 Véanse GONZÁLEZ RUS, "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicios y otros comportamientos semejantes", p. 248; o MORÓN LERMA, "Derecho Penal y nuevas tecnologías: panorama actual y perspectivas futuras", p.114.

9 Así, por ejemplo, GONZÁLEZ RUS, "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicios y otros comportamientos semejantes", pp. 248 y ss.; GUTIÉRREZ FRANCÉS, "Delincuencia económica e informática en el nuevo Código Penal", pp. 291 y ss.; o ROMEO CASABONA, "Los delitos de daños en el ámbito informático", p. 91.

10 Subraya MORILLAS FERNÁNDEZ, *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las*

II. Subsunción de los daños informáticos en el art. 263 del Código Penal: el tipo básico de daños en la propiedad ajena

A los daños informáticos obviamente no se ha referido hasta fechas recientes nuestro Código Penal. La cuestión es si la tradicional redacción que se contiene en el art. 263, tipo básico de las conductas de daños del Capítulo IX del Título XIII del mismo, permite o no abarcar esta clase de conductas cuando el objeto del ataque lo es no el componente físico del sistema, sino su componente lógico, o incluso cuando siéndolo el componente físico se afecta, además, la funcionalidad del sistema, lo que haría innecesarias previsiones específicas, salvo que se entendiera que la penalidad propuesta es insuficiente[11].

En su concepción tradicional el delito de daños ha venido exigiendo que el objeto sobre el que recae la conducta típica sea "cosa ajena o propia, mueble o inmueble, material y económicamente valorable, susceptible de deterioro o destrucción y de ejercicio de la propiedad"[12]. Será especialmente el carácter "corpóreo" o "material" que se exige de la "cosa" dañada el que plantee problemas de tipificación[13], pues estamos ante una característica que obviamente no tienen los elementos lógicos de un sistema informático, que son en realidad impulsos electromagnéticos, en su caso, incorporados a un soporte.

El ataque al *hardware* en principio no plantea mayores problemas de tipificación, con independencia de la resolución de cuestiones que tienen que ver sobre todo con la magnitud del

---

modalidades comisivas relacionadas con Internet, p. 108, que es incorrecto el uso del término sabotaje informático únicamente para los ataques a elementos lógicos de un sistema informático.

11 Véase ya, por todos, ROMEO CASABONA, *Poder informático y seguridad jurídica*, p. 176.

12 En estos términos, por todos, JORGE BARREIRO, "El delito de daños en el Código penal español", p. 513, incluyendo el daño en lo propio, reconducible al vigente art. 289.

13 Véanse, por ejemplo, MUÑOZ CONDE, *Derecho Penal. Parte especial*, p. 476; o QUINTERO OLIVARES, *Comentarios a la parte especial del Derecho Penal*, pp.749 y ss.

perjuicio causado o la especial dañosidad del ataque al margen de lo que en sí es el valor del bien dañado o incluso al hecho de que los daños puedan descubrirse al cabo de bastante tiempo[14]. Pero puede ocurrir que el daño al *hardware* implique el menoscabo de elementos lógicos del sistema y entenderse que el desvalor de la conducta no está suficientemente abarcado por la pena de los daños que se establezca en función del valor del elemento físico perjudicado. Y puede ocurrir que sin dañar en absoluto los componentes físicos del sistema informático se destruyan —o inutilicen o simplemente dañen o alteren— componentes lógicos del mismo[15].

Puede entenderse que el daño en los elementos lógicos del sistema conlleva una modificación de su soporte y que, por tanto, daña su sustancia impidiendo al *hardware* ser funcional o serlo en la misma manera en que lo venía siendo hasta la fecha —o, al menos, su valor real—, lo que permitiría acudir en estos supuestos a los tradicionales delitos de daños[16]. En la misma línea, puede entenderse que funcionalmente se perjudica el uso de dicho hardware cuando el mismo no le reporte a su propietario la utilidad pretendida y que, conforme a un concepto funcional, material o sustancial de la propiedad, el daño se ha producido aun cuando el valor económico (contable) del objeto afectado no se vea mermado (lo que ocurrirá cuando tras un lapso de tiempo pueda volver a utilizarse de modo plenamente satisfactorio) [17].

---

14 Alude a éstas y otras cuestiones CORCOY BIDASOLO, "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", p. 1001.

15 Lo plantean ya tempranamente autores como CORCOY BIDASOLO, "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", p. 1001; GONZÁLEZ RUS, "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", pp. 138 y ss.; o ROMEO CASABONA, *Poder informático y seguridad jurídica*, pp. 175 y ss., y "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías", pp. 179 y ss.

16 Así, por ejemplo, CORCOY BIDASOLO, "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", p. 1013.

17 Ampliamente, DE LA MATA BARRANCO, *Tutela penal de la propiedad*, pp. 77 ss.

Y puede entenderse también que el delito de daños no exige corporeidad en su objeto material, requisito aceptado sin apenas discusión en la explicación dogmática de sus características, pero que ciertamente no aparece en los preceptos dedicados a estos delitos y que en realidad es más propio de los delitos de apoderamiento o apropiación, que exigen la aprehensión de un objeto[18].

La subsunción de la conducta de daños, ante tales posibilidades, conduciría al art. 263 o al art. 625 en función de cómo se valorara el valor del objeto dañado: mayor o menor de cuatrocientos euros.

De una u otra manera puede intentarse dar cabida a los ataques al *software* de un sistema atendiendo una interpretación de los tipos tradicionales de daños —en el caso español, los arts. 263 y 625—, si se quiere, atenta a la realidad social del tiempo en el que han de ser aplicados[19], lo que no parece desacertado; pero siempre que asumiéramos un concepto funcional de propiedad, que atendamos más que a la incolumidad de la sustancia de una cosa a la de su valor de uso real, que prescindamos de la exigencia (no explícita típicamente) de la corporeidad del objeto sobre el que ha de recaer el daño y que, además, aceptemos la punición de daños "temporales" de los sistemas lógicos (o imposibilidad de uso de los mismos), la existencia del tipo penal sin daño físico (pero con imposibilidad de utilización, temporal o definitiva) y que entendamos que la pena prevista satisface el desvalor de la

18 Véanse, entre otros, BUENO ARÚS, "El delito informático", p. 5; GONZÁLEZ RUS, "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", pp. 139 y ss.; o ROMEO CASABONA, *Poder informático y seguridad jurídica*, pp. 176 y ss., o, posteriormente, "Los delitos de daños en el ámbito informático", p. 104.

19 En este sentido, los propios BUENO ARÚS, "El delito informático", p. 2; GONZÁLEZ RUS, "Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (art. 264.2 Cp)", pp.1285 y ss.; o ROMEO CASABONA, "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías", pp. 104 s.

conducta enjuiciada, sin atender cualquier otro tipo de lesividad que exceda lo que es en sí el ataque a una propiedad ajena de un valor concreto. Por todos estos matices que habría que efectuar para poder asumir la subsunción de los daños en los elementos lógicos de un sistema en el art. 263 (o en el art. 625), lo cierto es que son muchas las voces que reclaman un tratamiento específico para este tipo de conductas que tenga en cuenta la peculiaridad del objeto material —ausencia de materialidad—, la peculiaridad de la conducta —no necesariamente de destrucción física— y la peculiaridad del perjuicio —casi siempre muy superior a lo que en sí pueda representar el valor del objeto del delito—, no siempre de naturaleza patrimonial o al menos no en el sentido en que viene entendiéndose este término (quizás incluso ni asumiendo planteamientos materiales o funcionales y no meramente jurídico-económicos).

Si los tipos tradicionales de daños permiten abarcar de modo completo el conjunto de conductas caracterizadas como de daño informático con la interpretación que acostumbra a efectuarse de sus elementos (en particular, el concepto de daño —pérdida de valor del objeto del delito y no sólo perjuicio por imposibilidad de utilizar temporalmente el mismo— y la delimitación de cómo ha de definirse este objeto material —corporeidad del mismo—) no haría falta tipificación específica alguna. Si, por el contrario, se entiende que esto no es así, habría que completar la redacción con nuevas modalidades delictivas que hagan referencia a todas las ideas de ausencia de disponibilidad de un "objeto" (o quizás sólo servicio), desaparición del mismo, destrucción, disminución de funcionalidad, imposibilidad de acceso, inutilización, menoscabo, todas ellas entendidas en sentido amplio. Pero, aun en este caso, habrá que cuestionarse si esta ampliación sería suficiente para cubrir la tutela deseada o habría, por el contrario, que buscar nuevas ubicaciones sistemáticas para las figuras que pretenden abordarse penalmente —quizás a sancionar más gravemente que el delito básico de daños, por la trascendencia para la vida diaria de lo que representa hoy las TICs— y con ello, en realidad, nuevos objetos de tutela.

III. Posibles lagunas de penalidad y necesidad de previsión específica: propuestas internacionales

La importancia que ha adquirido este tipo de delincuencia ha motivado ya posicionamientos concretos en el ámbito supraestatal sobre el modo de afrontar la misma. Refiriéndonos a los dos Textos que en el ámbito europeo han tenido especial trascendencia en esta materia, tanto el Convenio sobre Cibercriminalidad de Budapest, del año 2001, como la Decisión Marco 2005-222-*JAI* del Consejo de Europa de 24 de febrero de 2005, relativa a los ataques de los que son objeto los sistemas de información, se ocupan de los daños informáticos.

El Convenio sobre Cibercriminalidad de Budapest contempla las conductas de daños informáticos en su artículo 4.1 bajo el epígrafe —y ya es sintomática la rúbrica— "atentados contra la integridad de los datos", obligando a los Estados firmantes a adoptar las medidas que resulten necesarias para convertir en infracción penal, conforme a su derecho interno, "el hecho, intencional y sin autorización, de dañar, borrar, deteriorar, alterar o suprimir datos informáticos". Otorga protección, por tanto, directamente, únicamente a los elementos lógicos —el *software*— de los sistemas informáticos —si bien no especifica cómo debe ser la modalidad de ataque— y contempla conductas que no implican necesariamente destrucción de un objeto, sino, simplemente, variación del contenido de un dato.

En el artículo 5, bajo la rúbrica "atentados contra la integridad del sistema", se contempla la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos, conductas que refieren los ataques de denegación de servicios o cualquier otra conducta con la que, por ejemplo, simplemente se ralentice el funcionamiento del sistema o se impida el acceso al mismo.

Y ni en uno ni en otro caso el tipo básico de daños de nuestro Código, en su interpretación al menos más tradicional, da cabida a las conductas descritas.

Un paso más se da, si cabe, en el artículo 6 del Convenio que requiere de los Estados firmantes adelantar la intervención penal para sancionar no sólo conductas contra datos o sistemas informáticos, sino, además, por un lado, la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de dispositivos o claves de paso concebidos o adaptados para permitir la comisión de los delitos que se describen en los artículos 2 a 5 del Convenio y, por otro, la mera posesión de estos dispositivos o claves de paso, aunque acepta que los Estados puedan exigir determinados requisitos para proceder a la sanción.

Por su parte, la Decisión Marco 2005-222-*JAI* del Consejo de Europa de 24 de febrero de 2005, relativa a los ataques de los que son objeto los sistemas de información, obliga a los Estados miembros, en su artículo 3, bajo la rúbrica "intromisión ilegal en los sistemas de información", a que prevean en sus ordenamientos la sanción de conductas realizadas sin autorización consistentes en "obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos". Gran amplitud, por tanto de conductas, que, a pesar de la rúbrica del precepto, exigen no sólo una intromisión ilegal en el sistema, sino un perjuicio a su funcionamiento.

El artículo 4 de la Decisión, que se ubica bajo el epígrafe "Intromisión ilegal en los datos" señala, con similares características, siguiendo la tónica del Convenio y diferenciando sistemas y datos contenidos en él, que "cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad".

De nuevo la distinción de artículos para referir conductas relativas al ataque a datos o a sistemas en una detenida descripción que abarca cualquier tipo de comportamiento en que en realidad

se afecte su integridad o disponibilidad —no la confidencialidad, que remite a otra problemática—, como acertadamente se dice en el Convenio, pero no justamente en la Decisión, que en la rúbrica alude a "intromisiones ilegales", lo que hace referencia a la idea de confidencialidad, seguridad en el uso, privacidad o uso libre de injerencias, más vinculada con otro tipo de conducta y otro tipo de interés.

Ése ha de ser a nuestro juicio el referente. El del perjuicio a la plena disponibilidad y posibilidad de utilizar un sistema (con sus programas, sus aplicaciones, sus datos), del que somos legítimos titulares, que nos permite desenvolvernos en nuestro entorno social como nosotros decidamos hacerlo.

IV. Subsunción de los daños informáticos en el art. 264.2 del Código Penal: tipo específico (agravado) de daños informáticos

1. Ubicación sistemática y bien jurídico a proteger: ¿el daño informático como delito patrimonial?

En el Código Penal, inmediatamente después del tipo básico de daños (art. 263), se prevé, como es sabido, una figura agravada en el art. 264.2 dedicada a la sanción de quien "por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos". Una figura que, dada su ubicación sistemática, puede entenderse como modalidad cualificada del tipo básico de daños —exigiendo por tanto que concurran, además de los propios, los elementos típicos del mismo—, dada su presencia junto a los tipos cualificados del art. 264.1 o bien como modalidad específica dado que el número 2 del artículo 264 no alude, como sí lo hace el número 1 a "los daños expresados en el artículo anterior", opción que parece más acertada, tanto por el tenor literal del precepto como por el contenido de su injusto. Pero sea desde una u otra perspectiva, lo que parece claro es que estaremos ante una infracción de carácter patrimonial.

En contra de esta ubicación se han levantado algunas voces críticas que consideran que la clase de conductas descritas en el precepto deberían regularse en un artículo ubicado en un capítulo independiente del de los daños en general. Así, se dirá, en realidad este nuevo delito —surgido en 1995— no es en realidad un subtipo del delito de daños sino una modalidad autónoma de daños a elementos lógicos[20].

Muchos otros autores, sin embargo, mantienen que estamos ante un subtipo agravado del delito de daños cuya ubicación es correcta[21], con el que el legislador, simplemente, ha pretendido zanjar las dudas que pudieran existir sobre la subsunción de estas conductas en el tipo básico —ésta sin duda es la razón de ser legal de este precepto, junto a la voluntad de agravar la pena (razón por la que puede haberse incluido en el art. 264), aun cuando con ella se obvia afrontar un debate de mayor calado en relación con lo que en el mismo ha de tutelarse realmente— y, al mismo tiempo, evitar la exigencia de comprobación de los elementos típicos del delito de daños cuando éstos se efectúen en elementos lógicos[22]; lo que, obviamente, obligaría a entender que estamos no ante un tipo cualificado sino ante un tipo autónomo agravado.

Ahora bien, ¿qué es lo que pretende protegerse cuando se aborda la sanción de conductas que, por afectarse los elementos lógicos de un sistema informático, menoscaban el correcto funcionamiento de éste, temporal o definitivamente (tal y como se exige desde los Textos internacionales)?.

---

20 Véanse ÁLVAREZ VIZCAYA, "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red", p. 277; ANDRÉS DOMÍNGUEZ, "Los daños informáticos en la Unión Europea", pp. 1726 y ss.; MORÓN LERMA, *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*, pp. 66 y ss.; o RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", pp. 280 y ss.

21 Entre otros, MARCHENA GÓMEZ, "El sabotaje informático: entre el delito de daños y los desordenes públicos", p. 358; MATA Y MARTÍN, *Delincuencia informática y derecho penal*, pp. 63 y ss.

22 Así, MATA Y MARTÍN, *Delincuencia informática y Derecho penal*, p. 80.

En la doctrina se ha mantenido, con carácter general, que el bien jurídico a proteger —al menos, el que se protege en el art. 264.2— es el mismo que cuando se sancionan conductas de daños sobre objetos corpóreos, materiales, físicos: la propiedad ajena[23]. El propio precepto, se dice, utiliza la expresión "ajenos" al referirse a los datos, programas o documentos objeto del ataque[24]. Llama en tal caso la atención que, siendo el objeto de protección el mismo, la pena sea mayor en este caso[25], lo que, es cierto, puede obedecer a razones vinculadas a la presencia de un mayor desvalor de resultado ajeno a la lesión de un bien jurídico distinto —o a una lesión mayor del patrimonio o del orden socioeconómico— o de acción, que no acostumbra a especificarse cuál es. Lo que sí parece evidente es que la naturaleza del precepto nada tiene que ver con la del resto de tipos agravados que contempla el art. 264 en su primer apartado, sin que esto, no obstante, sea óbice para su agrupación legal a partir de una necesidad de agravación —habría que concretar cuál— fundamentada en diferentes desvalores.

Sin embargo, son ya varias las voces que discrepan de esta postura. Y así, por ejemplo, se señala que podrá existir un sujeto que tenga un derecho de propiedad sobre el *hardware* en que se encuentren los datos objeto de ataque o, incluso, a veces, ciertos derechos de propiedad intelectual sobre algunos programas o bases de datos, pero no sobre los datos contenidos en el sistema[26],

---

23 Por todos, ORTS BERENGUER, E./ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, pp. 81 y ss.

24 Véase MATA Y MARTÍN, *Delincuencia informática y Derecho penal*, p. 80.

25 Como reconoce, aun manteniendo que el objeto de protección es el mismo, CHOCLÁN MONTALVO, "Fraude informático y estafa por computación", p. 314. Insiste, sin embargo, en que lo único que pretende el legislador es adaptar el articulado del Código a nuevas modalidades de comisión delictiva; podría haber creado delitos autónomos pero al abordar los delitos que tienen que ver con la informática señala el autor que el legislador ha optado por seguir protegiendo los bienes tradicionales de modo disperso a lo largo del Código. Así parece, efectivamente, que se ha procedido hasta ahora.

26 Así, RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", pp. 280 y ss.

con lo que no podría ser sujeto pasivo del delito de daños cometido sobre éstos y, desde esta interpretación, no podría hablarse de daños a la propiedad ajena; téngase en cuenta, sin embargo, que en los delitos patrimoniales basta con comprobar la ajenidad de la cosa para apreciar el tipo correspondiente, sin necesidad de acreditar quién sea el titular de la misma. O bien se indica que lo que realmente se protegen son intereses de contenido económico, que no hay que identificar con el patrimonio en sentido estricto[27] pues cuando se ejecuta una conducta de esta naturaleza las consecuencias económicas principales y más graves no se limitan a la de la pérdida del valor económico de los datos afectados, sino que se expanden al perjuicio para, por ejemplo, la actividad empresarial que se esté llevando a cabo[28]. Algo que, no obstante, se podría tener en cuenta en sede de responsabilidad civil[29].

Este tipo de inconvenientes que puede plantear mantener una concepción sobre lo que se trata de proteger con la sanción de este tipo de conductas centrada en la tutela del patrimonio de un sujeto —o de intereses de carácter socioeconómico a concretar— ha motivado nuevas posturas que aluden como objeto de tutela —en ocasiones, refiriéndose al conjunto de

---

27 Véase MORÓN LERMA, *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*, p. 67.

28 En este sentido, GUTIÉRREZ FRANCÉS, "Delincuencia económica e informática en el nuevo Código Penal", pp. 297 y ss.; o MATELLANES RODRÍGUEZ, "Algunas notas sobre las formas de delincuencia informática en el Código Penal", p. 142.

29 Señala MATA Y MARTÍN, *Delincuencia informática y Derecho penal*, pp. 78 y ss., que este tipo de postura es errónea al entender que el perjuicio del hecho delictivo no puede computarse para apreciar el delito de daños, pues lo que en éste se pretende tutelar no hace referencia a una cuantía económica como forma de menoscabo patrimonial, sino a la falta de disposición del propietario sobre sus bienes en todas sus dimensiones jurídico económicas. Siendo cierto (véase sobre el concepto funcional de propiedad —o patrimonio— y lo que éste implica, ampliamente, DE LA MATA BARRANCO, *Tutela penal de la propiedad y delitos de apropiación*, pp. 77 y ss.), también lo es que la comprobación del delito siempre exigirá concretar el valor funcional del objeto dañado (o apoderado, apropiado, etc.) y no el perjuicio causado.

delitos informáticos— a la información y la accesibilidad a la información[30], la accesibilidad y la integridad de la información y de los sistemas informáticos[31], simplemente la información[32], la seguridad de los sistemas informáticos, entendida como el derecho a no sufrir injerencias externas en los datos, programas o sistemas informáticos, por la trascendencia que éstos tienen para el desarrollo mundial[33], la comunicación pacífica a través de las redes telemáticas, con independencia, se dirá, de las garantías y protección que pueden ofrecerse a otros bienes jurídicos como la intimidad o la protección a datos de carácter personal[34], la confianza en el funcionamiento de los sistemas informatizados, como interés de carácter supraindividual, de los que dependen todas las actividades tanto públicas como privadas[35] o incluso, directamente, la tecnología de Internet, bien jurídico, se dirá, de primera magnitud[36].

Un aspecto importante a tener en cuenta es ciertamente el hecho de que la consolidada implantación de las TICs en prácticamente todos los ámbitos públicos y privados de la vida actual conlleva que un problema en las mismas implique, como antes se decía, consecuencias abrumadoras: desde la paralización de

---

30 Así, ÁLVAREZ VIZCAYA, "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red", p. 277.

31 En estos términos, RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", p. 281.

32 Así, LÓPEZ ORTEGA, "Intimidad informática y derecho penal (la protección penal de la intimidad frente a las nuevas tecnologías de la información y comunicación)", p. 117, considerando que estamos ante un bien de carácter supraindividual común a todos los delitos vinculados con la informática.

33 Véase MORILLAS FERNÁNDEZ, *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comisivas relacionadas con Internet*, pp. 109 y ss.

34 ROMEO CASABONA, "Los datos de carácter personal como bienes jurídicos penalmente protegidos", pp. 189 y ss., cauteloso con la intervención del Derecho Penal en esta materia.

35 Así, CORCOY BIDASOLO, "Problemas de la persecución penal de los denominado delitos informáticos", p. 10, señalando que ello explicaría el adelantamiento en la punición de algunos actos preparatorios.

36 De modo contundente, QUINTERO OLIVARES, "Internet y propiedad intelectual", p. 375.

un sistema del que puede depender toda una empresa hasta la de ordenadores públicos que cause un colapso en la Seguridad Social o la Policía.

Y la cuestión es la de si de lo que se trata es de proteger la propiedad (aun entendida desde una perspectiva funcional) o algo más. Claro que lo dañado han de ser los datos, documentos o programas contenidos en sistemas informáticos, como se reclama desde las Instancias internacionales y como el propio legislador español acoge. Por supuesto que el concepto tradicional de daños, centrado en la destrucción de una cosa, o los conceptos más elaborados que aceptan también el daño cuando la cosa desaparece o cuando definitivamente pierde su utilidad o valor de uso, han de ser revisados, porque lo que importa es que se pueda acceder a tales datos, que se pueda disponer de ellos, en todo momento y, además, de modo íntegro, no que su valor teórico (su sustancia) quede incólume. Pero, ¿con el fin de proteger la propiedad de quien tiene la capacidad de actuar con ellos?.

No se trata de entender que se protege la información contenida en soportes informáticos porque tenga más valor en sí misma que otra información contenida en otros soportes[37], pero sí que ello se hace por la importancia que tiene individual y socialmente su integridad y accesibilidad al estar situada en redes o sistemas informáticos de los que hoy en día dependen todos los ámbitos públicos y privados, más allá del daño al dato o sistema concretos.

Es de alguna manera lo que pretende afirmar el Convenio sobre Cibercriminalidad al ubicar en su Título 1 de la Sección 1 de su Capítulo II todas las conductas que atenten contra la "confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos", característica común de gran parte de los delitos informáticos; o incluso de todos si distinguimos entre

37 Es la crítica de GONZÁLEZ RUS, "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", p. 25.

Estudios Penales y Criminológicos, vol. XXIX (2009). ISSN 1137-7550: 311-362

delitos informáticos o contra sistemas informáticos y delitos cometidos a través de la informática[38].

En el caso español el art. 264.2 atendería —en su caso— los aspectos de integridad y disponibilidad; no el de confidencialidad, que habría que remitir —en su caso— al artículo 197 vinculado a la intimidad.

Sin embargo, criticando que el bien jurídico del art. 264.2, en los supuestos que se acogen en él, sea alguno de los anteriores y no la propiedad, se señala que al afirmar que se protege la información al margen de su significación económica, habría que castigar cualquier destrucción o menoscabo de la misma, aun sin significación económica, en contra de lo que se deduce del principio de intervención mínima, que carecería de sentido la distinción entre los daños superiores a los cuatrocientos euros de que habla el texto español y los que no desbordan esa cifra, que se excluiría la aplicación del delito de daños imprudentes —que exige siempre superar una determinada cantidad (en nuestro caso, ochenta mil euros)— o, en general, que prescindiéndose del valor del objeto material del delito o, al menos, del perjuicio patrimonial causado por la conducta típica, no tendría sentido la ubicación del delito entre los que vulneran la propiedad ajena[39]. Consideraciones frente a las que se alega que en realidad el hecho de que los daños informáticos lesionen o pongan en peligro la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos no impide que, al mismo tiempo, se vulnere la propiedad u otro tipo de intereses de carácter económico; las conductas que describe el art. 264.2 tendrían, en este sentido, carácter pluriofensivo[40]. En otros términos se dirá también que

---

38 Véase expresamente RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", pp. 260 y ss.

39 GONZÁLEZ RUS, "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", pp. 24 y ss.

40 Así, RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", pp. 261 y ss. ROVIRA DEL CANTO, *Delincuencia informática y fraudes informáticos*, pp. 71 y ss., habla de un delito pluriofensivo en el que junto a bienes jurídicos tradicionales individuales o colectivos, aparece un nuevo y

cuando se daña algún componente de un sistema informático no sólo se produce un daño en éste, sino que sus efectos se extienden a otros bienes jurídicos que se ven dañados ante este funcionamiento incorrecto del sistema informático[41].

Existe confusión, gran confusión sin duda, sobre lo que se quiere proteger cuando se penalizan los daños de carácter informático. Y a ella sin duda contribuye tanto el propio legislador, cuando redacta el art. 264.2 y cuando opta por una ubicación sistemática que obliga a considerar exclusivamente el aspecto patrimonial de la conducta, como la doctrina, que mantiene un concepto de propiedad y patrimonio que responde muy insatisfactoriamente a las nuevas realidades de lo que significa la posibilidad de desarrollo desde los espacios que garantizan unos datos, programas y sistemas informáticos cuando se puede acudir a los mismos sin injerencias de ningún tipo que perjudiquen la posibilidad de su uso (que es en definitiva lo que ha de garantizar la tutela patrimonial sobre determinados "bienes") .

Tal vez con la creación del art. 264.2 se pretende simplemente colmar lagunas de penalidad surgidas con una interpretación estricta y tradicional del delito de daños que impide subsumir en él muchas de las conductas de daño informático referidas. Seguramente. Tal vez se pretende ir más allá y proteger la información, en su vertiente de integridad y accesibilidad de la misma, para proteger no tanto el orden económico estricto cuanto el orden socioeconómico en sentido amplio; si se quiere, incluso a través de la protección de ciertos ataques al patrimonio individual. También habrá algo de esto. Podría explicarse así la ubicación del precepto, su penalidad agravada —explicada incluso por algún autor aludiendo a la pluriofensividad de estas conductas— e incluso, si se sostiene esta posición, la posibilidad

---

más importante bien jurídico de carácter supraindividual que es la información como bien y valor económico o social, quedando como bien secundario la integridad de los datos concretos dañados.

41 MARCHENA GÓMEZ, "El sabotaje informático: entre los delitos de daños y desordenes públicos", pp. 358 y ss.

de entender acertada la restricción de la sanción sólo para daños superiores a una determinada cantidad de dinero (por ejemplo, cuatrocientos euros) considerando que aunque lo trascendente no es el daño sino la potencialidad para vulnerar intereses de carácter supraindividual —se definan de uno u otro modo— la conducta típica debe tener cierta entidad que puede venir dada por esa limitación, que, en todo caso, no obstaría a la sanción como falta de todo tipo de conductas dañosas.

Pero el debate sobre cuál sea el objeto protegido en el art. 264.2 es un debate forzado porque surge de una previsión legal precipitada en la que no se tuvo información suficiente para reflexionar sobre lo que había que proteger. El fenómeno de la delincuencia informática, los pronunciamientos internacionales sobre la necesidad de nuevos tipos penales, la propia discusión de la doctrina destacando las insuficiencias de la regulación vigente motivó un precepto que lo lógico es que en su momento se ubicara donde se hizo por la connotación de destrucción o menoscabo que implica el concepto de daño. Pero la reflexión posterior a la hora de explicar su bien jurídico, las insuficiencias de una consideración estrictamente económico-patrimonialista del precepto atenta más a la pérdida de valor de la cosa que a la pérdida de valor de su funcionalidad —ya por lo que entonces queda sin tutelar, ya por la ausencia de atención a perjuicios de especial consideración— o la dificultad de definir la naturaleza del nuevo precepto como tipo cualificado o como tipo autónomo han ido dando unas pautas que obligan a plantearse qué es lo que en realidad perjudican los daños informáticos.

Y aquí surge la necesidad de investigación sobre la posibilidad o necesidad de tutelar como bien autónomo, al margen de lo que sea que tutele el art. 264.2, cuya ubicación sistemática obliga a entenderlo patrimonialmente —aunque no desde la trasnochada concepción jurídico económica, que aquí muestra sus insuficiencias, sino desde una perspectiva funcional—, la integridad y disponibilidad de la información contenida en redes o soportes informáticos, que tiene que ver con un concepto funcional de propiedad y patrimonio, pero que va algo más allá de lo que éste

trata de explicar. Que dicha tutela tenga que atender consideraciones sobre el menoscabo al correcto desarrollo socioeconómico es quizás excesivo. Sin duda, puede estar presente como razón de ser del precepto —de modo mediato, difuso—: garantizar un instrumento (las TICs) básico en todo proceso socioeconómico de la vida actual; pero quizás sólo eso, porque esa integridad no se protege sólo, ni siquiera prioritariamente, para garantizar dicho desarrollo, sino para preservar una actuación individual muy menoscabada —al margen de cuestiones de confidencialidad, intimidad, privacidad o seguridad, que han de quedar al margen de lo que es estrictamente el "daño" informático y reconducirse a la idea de intromisión— de afectarse la posibilidad de disponer en todo momento, de modo íntegro y con plena funcionalidad operativa, de los datos, programas y sistemas con los que operamos en nuestra vida, privada o pública, diaria.

2. Análisis del tipo objetivo

A) Conducta típica

El art. 264.2 sanciona a quien "por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

La expresión "por cualquier medio", en técnica de *numerus apertus*, abre la posibilidad de comisión del delito a cualquier clase de acción idónea para causar el daño que refiere el precepto[42]. Tanto, y en ello se insistirá posteriormente, en relación a ataques físicos a los soportes lógicos en que esté contenida la información

42 En este sentido, FERNÁNDEZ PALMA/MORALES GARCÍA, "El delito de daños informáticos y el caso Hispahack", p. 1524; también, RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", pp. 282 y 283, afirman que la enumeración de verbos que se hace en el artículo 264.2, es meramente ejemplificativa de los posibles modos de comisión, dada la peculiaridad del objeto material de este delito de daños informáticos que hace que los daños puedan consistir además de en la destrucción de la cosa, en su inutilización o en su alteración.

afectada como en relación con procedimientos de naturaleza informática que permiten el acceso físico o a través de la Red al sistema para, directamente, causar el daño referido.

Así, por ejemplo, cuando los daños informáticos se cometen a través de Internet, su autor puede introducirse en el sistema para destruir, alterar o dañar datos, programas o documentos. Puede también introducir en el sistema virus, troyanos, gusanos o cualquier otro programa o rutina nocivos. Y puede también, sin introducirse en el sistema, interceptar los archivos o datos que están siendo transferidos a través de la red para dañarlos. En todo caso, la rápida evolución que sufren las nuevas tecnologías puede favorecer nuevas modalidades que faciliten menoscabos a las mismas y, en este sentido, una regulación demasiado descriptiva de los modos en que han de ser dañados los elementos lógicos de los sistemas informáticos podría dejar fuera, en muy poco tiempo, toda clase de nuevas conductas lesivas en este ámbito[43]. De ahí lo acertado del texto del Código en cuanto al énfasis que pone en el resultado dañoso más que en el procedimiento a través del cual se causa el mismo.

Más compleja es la interpretación de cuál es el resultado al que ha de conducir la conducta típica, de qué ha de entenderse por "daño" en este precepto y de si la destrucción, alteración, inutilización o "daño", como concepto envolvente de los anteriores, según acepta el propio texto con la expresión "de cualquier otro modo", refiere la pérdida de la sustancia del objeto material o la de su "valor real" (mejor sería hablar en la actualidad de pérdida de funcionalidad), siguiendo la terminología tradicional.

Considerando este precepto como un subtipo del delito de daños y sin separarse de la concepción tradicional en la

---

43 ROMEO CASABONA, "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal", pp.12 y ss., afirma que los tipos creados por el legislador para recoger la criminalidad informática no deben apoyarse en la descripción exhaustiva de las características técnicas de la acción para evitar que la rápida evolución técnica deje los artículos desfasados en un corto plazo de tiempo.

interpretación del mismo, que exige un menoscabo material de su objeto material, en ocasiones se ha señalado que los elementos lógicos de un sistema son "cosas" a estos efectos, igual que lo pueden ser los componentes físicos de un equipo informático y que cualquier afección a los datos del sistema implica el menoscabo de su sustancia[44].

La destrucción de datos, programas o documentos es posible sin duda, tanto dañándose los soportes o circuitos que los contienen como haciendo desaparecer archivos. Sin embargo, lo cierto es que las propias características de los elementos lógicos de un sistema informático hacen que resulte muy difícil saber cuándo la sustancia, teniendo en cuenta que nos hallamos ante cosas inmateriales, ha sido dañada o en qué medida lo ha sido. Lo que en cambio no podrá negarse es que la funcionalidad del sistema se menoscaba cuando se atacan los datos o programas de los sistemas informáticos[45] y que el propio Código confirma la existencia de un daño en tales casos tanto cuando acude en el dictado típico del precepto al verbo "inutilizar"[46], porque inutilizar no es sino hacer imposible la utilización de lo que se menoscaba

---

44 GONZÁLEZ RUS, "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", pp. 140 y ss.

45 En términos parecidos, FERNÁNDEZ PALMA/MORALES GARCÍA, "El delito de daños informáticos y el caso Hispahack", p. 1534, entienden que el daño a considerar debe ser el funcional, atendiendo a la utilidad concreta que estos datos, programas o documentos tengan para el propietario, siendo el valor del perjuicio el que contiene la verdadera lesividad material de la conducta; en el mismo sentido, MATA Y MARTÍN, *Delincuencia informática y derecho penal*, pp. 71 y ss. En contra, FERNÁNDEZ TERUELO, *El cibercrimen, los delitos cometidos a través de Internet*, pp. 114 y ss., considera que el daño funcional se aproxima demasiado al perjuicio y que no debe computarse éste sino los costes de recuperación de los datos, entendiendo realizado el tipo si esta recuperación fuese imposible.

46 En este sentido, MATA Y MARTÍN, "Criminalidad informática: una introducción al cibercrimen (1)", p. 11; anteriormente, ya ROMEO CASABONA, "Los delitos de daños en el ámbito informático", p. 107. En contra GONZÁLEZ RUS, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", pp. 5 y ss.

conforme a su uso habitual, como cuando concluye con la expresión "de cualquier otro modo dañe".

Más compleja aún es la interpretación de la expresión "alterar". Así, por ejemplo, ¿se comete el delito añadiendo nuevos datos a los ya existentes de tal manera que los datos iniciales siguen presentes pero junto a otros nuevos?. Parece que sí si la introducción de datos nuevos en el sistema lo hace inútil para un determinado uso original, pero difícilmente si se añaden datos que no perjudican su funcionamiento, aunque se haya producido una alteración. Téngase en cuenta que el precepto alude a la destrucción, alteración o inutilización como sinónimos del daño.

Si la alteración debe ser definitiva o no es algo que el precepto no especifica. Tampoco se especifica en relación con la inutilización (la destrucción siempre implica menoscabo definitivo —total o parcial— del objeto dañado).

En la interpretación tradicional del delito de daños, cuando el objeto afectado puede volverse a utilizar de modo absolutamente similar a como se usaba antes del ataque producido, sin pérdida de su sustancia ni de su funcionalidad, nadie afirmaría la tipicidad del mismo, a pesar del posible perjuicio sufrido, a resarcir por vía civil[47]. La cuestión es si con ello se satisfacen los compromisos internacionales adquiridos y se atiende la realidad actual y el hecho innegable de que puede ser mucho más importante (y por tanto más atendible en sede penal) una imposibilidad temporal de utilización del sistema de cierta entidad que un mínimo menoscabo permanente de algún dato del sistema.

A este respecto, piénsese, por ejemplo, en las conductas de denegación de servicios de carácter transitorio.

Estos ataques de denegación de servicios consisten en agresiones que impiden el uso legítimo de un sistema informático

47 FERNÁNDEZ TERUELO, *El cibercrimen, los delitos cometidos a través de Internet*, p. 113, opina que al contemplar el tipo la conducta de alterar, puede subsumirse en él no sólo la pérdida de datos total o parcial, sino también el impedir temporal y/o definitivamente su utilización, incluyendo, por ejemplo, la ralentización del sistema.

o de alguno de sus recursos. Se realizan por medios informáticos saturando de información el sistema e inutilizando temporalmente el mismo o alguno de sus recursos limitados. La característica de estos ataques es que no sólo pueden realizarse mediante introducción de rutinas nocivas que supongan una alteración de datos —que tendría cabida por ello mismo en el precepto—, sino que también pueden realizarse a través de técnicas que no supongan ninguna modificación de datos o programas (por ejemplo, en casos de petición masiva de información a un sistema, que posteriormente no se acepta con la consiguiente saturación de éste)[48].

A pesar de que muchas de estas conductas pueden ser de mucha gravedad —piénsese en el caso extremo del bloqueo durante un mes de la página *Web* de una empresa que sólo opera a través de Internet— y que sería conveniente adecuar el precepto para incluir al menos los casos más graves de denegación de servicios, tal y como se demanda desde las instancia internacionales con toda lógica, difícilmente puede entenderse que los datos o programas estén dañados en su sustancia o funcionalidad si la alteración o inutilización no es definitiva. Y en tal caso menoscabos temporales debieran quedar al margen del precepto —en su actual ubicación sistemática—, al igual que ocurre en las figuras de hurto o apropiación indebida con los usos temporales no expropiatorios.

Sin embargo, y en sentido opuesto, todo acceso a los datos, programas o documentos electrónicos de redes, soportes o sistemas implica una mínima modificación de los mismos —una alteración, por tanto— y, con ello, la realización del tipo. ¿Debe entenderse típica toda alteración de un *software* o sólo aquélla que difiera de las alteraciones derivadas del uso normal del mismo, esto es, sólo aquélla que conlleve un menoscabo del objeto, sea en su esencia sea en su funcionalidad?. Esto último sería más coherente con el bien a proteger[49].

---

48 Véanse RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", p. 279.

49 Mantienen esta última posición FERNÁNDEZ PALMA/MORALES GARCÍA, "El delito de daños informáticos y el caso Hispahack", pp. 1525 y 1526.

Por otra parte, ¿habrá de exigirse un "daño" superior a 400 euros, como se requiere para la aplicación del art. 263, lo que excluiría del art. 264.2 estas modificaciones producidas con el uso normal del sistema o, dado el silencio del precepto a este respecto —y entendiendo el mismo como tipo específico y no meramente cualificado—, no es necesaria esta exigencia?. Esto último es más coherente con el tenor literal del precepto y con las propuestas internacionales y, además, tiene en cuenta la dificultad de cuantificar en cuanto a lo que es su sustancia el valor de un dato o de un archivo[50] y dota de mayor tutela a los elementos lógicos del sistema; aunque ciertamente plantea numerosos problemas cuando lo que se dañan son éstos a través del menoscabo del *hardware*. Ello, por supuesto, al margen de cuál sea el perjuicio que pueda experimentar el titular de los datos, programas o sistemas informáticos, que sólo interesa tener en cuenta para constatar la tipicidad de la conducta en cuanto el mismo se derive directamente del menoscabo de éstos[51].

En cuanto a la posibilidad de comisión de estos delitos por omisión, obviamente hay que descartar la omisión propia, pero no la impropia[52]. Así, por ejemplo, cuando los operadores —en posición de garantía— puedan tener conocimiento de que desde sus servidores se pueden estar cometiendo delitos de daños, pero,

---

50 En el primer sentido, entre otros, GONZÁLEZ RUS, "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes", p. 268; en este último, FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet*, p. 113, explicando que un sistema informático es una síntesis entre el *hardware* y el *software* y el bloqueo del mismo implica una alteración del funcionamiento de uno o varios programas, programas que son recogidos específicamente como objeto material del delito; también RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", p. 283.

51 Véase MATA Y MARTÍN, *Delincuencia informática y derecho penal*, p. 73. En este sentido hay que entender la exigencia de perjuicio para el sujeto pasivo que reclaman SERRANO GÓMEZ/SERRANO MAILLO, *Derecho penal. Parte especial*, p. 469.

52 Así, MATA Y MARTÍN, *Delincuencia informática y derecho penal*, p. 69.

sobre todo, cuando sabiendo que se ha introducido una bomba lógica que se activará porque se ha rescindido, por ejemplo, un contrato de mantenimiento del sistema informático, no impiden la destrucción operada por el *software* malicioso[53].

Finalmente, antes se aludía a la posibilidad de que los daños a los elementos contenidos en redes, soportes o sistemas se realizaran mediante ataques al *hardware* y no directamente al *software*.

El legislador español, diferenciando el daño en los elementos materiales de un sistema, que sanciona en el tipo básico de daños del art. 263, y los daños en sus elementos lógicos, que sanciona en el tipo agravado del art. 264.2, obliga a cuestionarse qué ocurre cuando la desaparición o disfuncionalidad de los segundos surge a través de la destrucción o menoscabo de los primeros o, simplemente, cuándo aplicar uno u otro precepto; teniendo en cuenta la diferencia de penalidad de ambos —importante además porque la pena de multa de un caso se convierte en prisión en otro—, al margen ahora de cuál sea la razón que fundamente la misma.

Las conductas de daños informáticos, en sentido amplio, pueden llevarse a cabo a través de ataques mediante la Red con los que el *hardware* puede quedar indemne —aunque realmente dicha indemnidad poco importará porque estaremos ante un continente sin contenido—, pero también pueden cometerse a través de ataques a los componentes materiales de un ordenador, de una central de datos, que implique la pérdida de éstos, la pérdida del *software*.

Obviamente cuando el ataque al *hardware* en absoluto afecte a los datos o programas contenidos en el sistema ni a su accesibilidad —por ejemplo, la destrucción de un altavoz, del micrófono o del ratón— estaremos ante un supuesto normal de daños reconducible al tipo básico. Sí podrá entenderse que

53 Detenidamente, CORCOY BIDASOLO, "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", p. 1011.

estamos ante unos daños informáticos si por tales entendemos el menoscabo de un componente (en este caso, material, físico) del sistema, pero la reparación es fácil, el perjuicio escaso (dependerá, claro, del importe en que se valore el objeto dañado) y realmente nada tiene que ver esta conducta con las que realmente se quiere evitar desde los textos internacionales cuando se aborda el problema del cibercrimen y se alude a la integridad o disponibilidad de datos y programas.

Si este ataque supone al mismo tiempo dejar inoperativos los elementos lógicos del sistema, por ejemplo, dañando intencionadamente la fuente de alimentación, de tal forma que resulta imposible acceder a los datos contenidos en el sistema, al menos hasta solucionar el problema en el hardware o extraer las placas de memoria del ordenador afectado e insertarlas en otro ordenador distinto, el problema es diferente. Habría que acudir al art. 264.2, que, como exigen los Textos internacionales, incorpora el término "inutilización" a su redacción típica. Cuestión independiente de si se ha producido un perjuicio superior a cuatrocientos euros o no, que, obviamente, habrá que comprobar si se entiende que ésta es una exigencia típica del art. 264.2 (no es ésta nuestra opinión); téngase en cuenta en todo caso que este perjuicio, directamente derivado del menoscabo producido, no se producirá nunca con inutilizaciones temporales (al margen del perjuicio indirecto que se pueda generar).

Y si el ataque, mediante el daño del *hardware*, destruye datos, programas o documentos contenidos en el mismo, habría que subsumir dicho ataque también en el artículo 264.2.

Ahora bien, en estos casos, de aplicar el precepto previsto para la sanción de los daños en elementos lógicos, ¿hay que sancionar también los daños en los elementos materiales del sistema de modo independiente (concurso de delitos) o podrá entenderse, por el contrario, que los mismos se entienden subsumidos en la pena prevista por el art. 264.2 (concurso de leyes, por especialidad o por consunción)?.

Un grupo de autores propone aplicar el art. 264.2 tanto cuando se produzcan directamente daños en el *software* como cuando se produzcan sólo daños en el *hardware*, siempre que en éste se contenga algún elemento lógico, aunque el mismo no se vea dañado[54]. Habría que entender para ello que el bien jurídico protegido en uno y otro precepto es el mismo, la propiedad y que se agrava la pena del segundo simplemente por encontrarnos ante elementos de naturaleza informática, físicos o lógicos. Pero si entendemos que lo que se tutela en el art. 264.2 no es la propiedad sino la información, la integridad de los datos, etc., un ataque al *hardware* que contenga elementos lógicos pero que no dañe dicha información o no la haga inaccesible no podría subsumirse en este precepto.

Otros autores entienden por ello que el art. 263 debe aplicarse cuando únicamente se dañe alguno de los componentes físicos del sistema informático y no sus componentes lógicos. Dañándose éstos, además del *hardware*, entienden que habría que aplicar únicamente el artículo 264.2[55], en base a una relación concursal de normas en la que este artículo es ley especial, computando los daños en uno y otro tipo de componente para calcular el valor total del daño, que se entiende ha de ser superior a los cuatrocientos euros[56]. El problema va a estar en el cálculo

---

54 Así, GONZÁLEZ RUS, "Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (art. 264.2 Cp)", pp. 1295 y ss.

55 En este sentido, MATA Y MARTÍN, *Delincuencia informática y derecho penal*, pp. 64 y 65, afirmando que lo relevante es que se produzca un determinado resultado de destrucción, deterioro, alteración o inutilización y no el modo en que este resultado se produzca. El propio precepto 264.2 señala, añade el autor, que pueden cometerse los daños "por cualquier medio"; por tanto, también a través de daños en los componentes físicos del sistema.

56 Así, GIMÉNEZ GARCÍA, "Delito e informática. Algunos aspectos de derecho penal material", p. 207; y ORTS BERENGUER/ROIG TORRES *Delitos informáticos y delitos comunes cometidos a través de la informática*, pp. 80 y 81. Téngase en cuenta sin embargo que el art. 264.2 no exige, al menos literalmente, que el daño exceda los cuatrocientos euros, interpretación doctrinal derivada únicamente de considerar el art. 264.2 tipo cualificado del art. 263, pero que no tiene en cuenta la peculiaridad del objeto material (ni la posible afectación de un bien jurídico distinto de la propiedad ni, en su caso, la pluriofensividad del delito).

del valor del daño y en que si éste —en elemento lógicos— se produce mediante un daño al *hardware* superior a cuatrocientos euros, aunque el daño a los elementos lógicos sea ínfimo, habría que aplicar para estos autores el art. 264.2, mientras que si el daño a los elementos lógicos surge por otra vía —y no supera los cuatrocientos euro— no cabría aplicar este precepto (si se considera tipo cualificado y no autónomo), debiendo aplicarse el art. 263 si, posteriormente, se realiza un ataque al *hardware*.

Podría opinarse, en cambio, que hay que acudir a un concurso de infracciones, pero ello obligaría a entender que estamos ante dos bienes jurídicos diferentes y que en el art. 264.2 no se tiene en cuenta en modo alguno la lesión de la propiedad ajena.

La cuestión va a depender simplemente de cuál se entienda es el bien jurídico protegido en uno y otro precepto. De entenderse que en ambos es la propiedad (el patrimonio), el concurso de normas es obligado, siendo siempre preferente el art. 264.2, que será a su vez aplicable cuando el daño en los elementos lógicos se produzca a través de cualquier medio que no sea el de destrucción de *hardware*, reservando el art. 263 sólo para cuando ésta no afecte en modo alguno al funcionamiento lógico del sistema (y, por la previsión legal española, se superen los cuatrocientos euros). De entenderse que el bien jurídico del art. 264.2 tiene naturaleza pluriofensiva, también será obligado el concurso de normas. Y aunque se mantenga como objeto de tutela la integridad o disponibilidad de datos o programas también habrá que acudir al concurso de normas dependiendo, claro, cómo se explique este nuevo objeto de tutela; pero si, como así parece debe ser, el mismo hace referencia a la posibilidad de disfrute personal, libre de intromisiones ajenas —descripción que habría que precisar— de los equipos informáticos que se poseen, el concurso de infracciones no sería posible.

B) Sujetos del delito

El artículo 264.2 exige la destrucción, alteración, inutilización o daño de datos, programas o documentos electrónicos

"ajenos". Esta necesidad de ajenidad del objeto material hace que el propietario de los mismos no pueda, obviamente, ser sujeto activo del delito[57]. Cuándo a estos efectos un objeto es propio o ajeno es algo que habrá que concretar atendiendo a la legislación sobre propiedad intelectual[58].

La posibilidad de encauzar las conductas en las que el propietario destruya datos, programas o documentos dentro del delito de realización arbitraria del propio derecho —por ejemplo, para impedir su utilización por parte de quien puede tener acceso a ellos por razones muy variadas (contratos legales de uso ya vencidos, etc.)— parece quedar descartada en los supuestos en que los ataques sean realizados a través de medios técnicos, pues requisito del art. 455 es que se actúe con violencia, intimidación o fuerza en las cosas[59]. La peculiaridad del objeto sobre el que recae el delito de daños informáticos podría requerir una adaptación de lo que se entiende por fuerza en las cosas para la aplicación de este art. 455, máxime si entendemos que la utilización de medios técnicos para dañar la propiedad ajena puede encajar perfectamente en el art. 264.2 (alteración, destrucción, inutilización), pero hoy en día, proponer una interpretación del concepto de fuerza que extienda el significado ya bastante amplio de este concepto rayaría la analogía prohibida.

Si bien el propietario no puede ser autor del delito del art. 264.2, puede darse, no obstante, el supuesto de que siendo el propietario del programa el que comete la acción de destrucción del mismo, que en principio resultaría atípica, se dañen datos contenidos en ese programa que no le pertenezcan a él sino a su

---

57 Señala CORCOY BIDASOLO, "Problemas de la persecución penal de los denominado delitos informáticos", p. 18, que es la ubicación de este precepto entre los delitos de daños la que no permite que sea el propietario sujeto activo del delito.

58 GUTIÉRREZ FRANCÉS, "Delincuencia económica e informática en el nuevo Código Penal", p. 298.

59 En este sentido, MATA Y MARTÍN, *Delincuencia informática y Derecho penal*, pp. 67 y 68; ROMEO CASABONA, "Los delitos de daños en el ámbito informático", p. 113.

poseedor o legítimo usuario, con lo que cumpliendo el resto de requisitos típicos, la acción sí sería constitutiva de este delito del artículo 264.2[60]. Cuando con el daño realizado por el propietario del programa se afecte a los datos que no son de su titularidad no podrá alegarse por parte del autor legítima defensa, aunque el poseedor esté, por ejemplo, realizando copias de un programa protegido por la legislación sobre propiedad intelectual. La destrucción de los datos no resulta inevitable y necesaria para evitar el ataque al derecho de propiedad intelectual; no estaríamos ante un medio racionalmente necesario para repeler la agresión ya que existen otras posibilidades técnicas para salvaguardar la titularidad. Sin embargo, sí cabría apelar a una legítima defensa incompleta[61]. En todo caso, lo normal será que los problemas derivados de este tipo de situación sean solventados en sede civil.

Por supuesto, no es necesario que el sujeto activo del delito conozca quién es el propietario de los elementos lógicos que daña para ser considerado autor del delito; basta, como ya se ha señalado, que los mismos no sean de su titularidad[62].

Finalmente, si se entiende que el bien jurídico protegido por este delito es la propiedad, y que por tanto nos encontramos ante una modalidad agravada del delito de daños, sólo podrá ser sujeto pasivo del delito el propietario. Los usuarios legítimos de los elementos dañados únicamente podrán ser sujetos pasivos de la acción y, en su caso, perjudicados[63]. Otra sería la postura a mantener, obviamente, de mantener posiciones sobre el bien

---

60 Lo señalan, ROMEO CASABONA, "Los delitos de daños en el ámbito informático", pp. 111 y ss.; y ROVIRA DEL CANTO, *Delincuencia informática y fraudes informáticos*, p. 235.

61 Véase, GONZÁLEZ RUS, "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes", p. 260; ROMEO CASABONA, "Los delitos de daños en el ámbito informático", p. 112.

62 GONZÁLEZ RUS, "El Cracking y otros supuestos de sabotaje informático", p. 233.

63 Por todos, GONZÁLEZ RUS, "Daños a través de Internet y denegación de servicios", p. 1477.

jurídico protegido por el delito que sobrepasen la estricta consideración patrimonial de éste.

C) Objeto material

El objeto material del delito de daños informáticos contemplado en el artículo 264.2 lo integran los "datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos".

En el momento del ataque el dato o programa dañado puede encontrarse en un soporte físico, como puede ser un CD, una memoria extraíble, un disco duro, etc., o puede estar siendo transmitido a través de una red. Lo característico de estos datos, programas o documentos electrónicos es, en todo caso, su naturaleza de impulsos electromagnéticos; no tienen una naturaleza corpórea y requieren ser procesados por algún sistema[64].

Su calidad de impulsos electromagnéticos que requieren ser procesados para su comprensión humana viene señalada en el Convenio sobre Cibercriminalidad de Budapest de 2001 y en la Decisión Marco del Consejo de Europa de 2005. El Convenio describe en su artículo 1.b) como datos informáticos, toda representación de hechos, de informaciones o de conceptos bajo una forma que se preste a un tratamiento informático, incluidos los dirigidos a permitir que un sistema informático ejecute una función. Quedan incluidos en esta definición dada por el Convenio tanto los datos como los programas informáticos. La Decisión Marco, también en su artículo 1.b), define estos datos como cualquier representación de hechos, informaciones o conceptos creada o dispuesta de tal forma que permite su tratamiento por un sistema de información, incluido un programa gracias al cual se permite a dicho sistema realizar una función.

Los datos son, en síntesis, unidades básicas de información que después de ser procesadas dan lugar a una "información".

64 En este sentido, MATA Y MARTÍN, *Delincuencia informática y Derecho penal*, p. 66.

Estudios Penales y Criminológicos, vol. XXIX (2009). ISSN 1137-7550: 311-362

El documento electrónico es el conjunto de datos creado tras su procesamiento informático.

El programa, según lo establece el art. 96.1 la Ley de Propiedad Intelectual, es la secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea, o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación. Esta misma ley en su párrafo segundo considera también programas a los efectos de la misma toda la documentación preparatoria, la documentación técnica y los manuales de uso de un programa, que, aunque programas a efectos de la Ley, quedan sin duda fuera de lo que es el objeto material del art. 264.2 del Código Penal.

Los datos, programas o documentos electrónicos deben encontrarse recogidos, dice este artículo, en "redes, soportes o sistemas informáticos".

Una red es el sistema constituido por numerosos ordenadores y terminales interconectados entre sí por canales de comunicación públicos o privados[65]. En alguna ocasión se ha hecho referencia a que el término "contenidas" utilizado por el artículo 264.2 es inadecuado para las redes informáticas, ya que éstas no contienen sino que transmiten datos, programas o documentos electrónicos[66]. Lo cierto es que ello no plantea mayor problema, ya que en realidad mientras se transmiten los datos a través de las redes, estos datos se contienen en las mismas.

Los soportes son los dispositivos físicos en donde se encuentran recogidos los ficheros, programas o documentos electrónicos, cualquiera que sea su naturaleza y funcionamiento (electromagnético, óptico, memora *RAM*, *ROM*, etc.)[67].

---

65 ELOSUA/PLÁGARO, *Diccionario LID tecnologías de información y comunicación*, p. 449.

66 Lo pone de manifiesto, GARCÍA GARCÍA-CERVIÓN, "Daños informáticos. Consideraciones penales y criminológicas", p. 11.

67 GONZÁLEZ RUS, "El Cracking y otros supuestos de sabotaje informático", p. 229.

El sistema hace un uso extenso de los ordenadores y otros dispositivos asociados para realizar sus funciones y operaciones[68].

Y la referencia al término "informático" debe entenderse en este contexto referida a cualquier conjunto de dispositivos físicos, ficheros y aplicaciones lógicas que permiten el procesamiento automático mediante combinaciones numéricas de, en este caso, datos, programas y documentos electrónicos[69].

Refiriéndose a la naturaleza de estos datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos, algún autor erróneamente ha señalado como compresivos de los mismos únicamente aquellos económicamente evaluables para la actividad empresarial, que afecten a la capacidad competitiva de una empresa[70]. Pero, es evidente que el artículo 264.2 no excluye de su protección la destrucción de los datos, programas o documentos electrónicos de particulares.

En cuanto a la cuantía del daño al objeto material del delito, un sector de la doctrina insiste, como antes decíamos, en la necesidad de que el mismo supere los 400 euros a que alude el art. 263. El argumento esgrimido por estos autores es el de que las diferencias punitivas que se generarían en caso contrario respecto a ambos delitos serían totalmente desproporcionadas sólo por encontrarnos ante un objeto material de naturaleza informática. Se añade también que el Código Penal sólo protege los datos cuando tienen un valor en relación a un bien jurídico determinado; siempre, por tanto, en dependencia de su valor económico o instrumental para la protección de otros bienes jurídicos[71]. El

---

68 ELOSUA/PLÁGARO, *Diccionario LID tecnologías de información y comunicación*, p. 447.

69 Así, GONZÁLEZ RUS, "Daños a través de Internet y denegación de servicios", p. 1475.

70 De esta opinión, MATELLANES RODRÍGUEZ, "Algunas notas sobre las formas de delincuencia informática en el Código Penal", p. 142.

71 Entre otros, GONZÁLEZ RUS, "Daños a través de Internet y denegación de servicios", p. 1476; y MATA Y MARTÍN, *Delincuencia informática y derecho penal*, p. 73.

límite económico de los 400 euros puede resultar necesario si se quiere garantizar el principio de mínima lesividad de la conducta enjuiciada, teniendo en cuenta para computar dicho daño, por supuesto, tanto la sustancia como la funcionalidad del objeto dañado[72], único modo de evitar que queden fuera del ámbito de aplicación del precepto conductas generadoras de daños verdaderamente importantes[73].

Pero otro sector doctrinal entiende en cambio, en postura más coherente con la literalidad del precepto, con lo que es el objeto del delito y con la voluntad agravatoria del legislador, que en el ámbito del artículo 264.2 no debe considerarse aplicable la cuantía mínima del daño a que se refiere el art. 263[74]. Dado que el legislador no prevé específicamente la necesidad de una cuantía mínima, como sí hace con el art. 263 y con el art. 264.1, debe entenderse que expresamente se excluye esa posibilidad. Aunque el primer número del art. 264 tome como referente el artículo 263, ello no implica que también lo haga el número segundo[75]. Máxime teniendo en cuenta que no estamos ante un tipo cualificado, sino específico, e incluso, para muchos, mal ubicado conjuntamente con el tipo básico de daños[76].

---

72 Comparten esta opinión CHOCLÁN MONTALVO, "Fraude informático y estafa por computación", p. 321; MATA Y MARTÍN, *Delincuencia informática y derecho penal*, p. 73; y ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, p. 81.

73 En este sentido también FERNÁNDEZ PALMA/MORALES GARCÍA, "El delito de daños informáticos y el caso Hispahack", p. 1527.

74 Así, ANDRÉS DOMÍNGUEZ, "Los daños informáticos en la Unión Europea", p. 1727; GUTIÉRREZ FRANCÉS, "Delincuencia económica e informática en el nuevo Código Penal", p. 298; MARCHENA GÓMEZ, "El sabotaje informático: entre los delitos de daños y desórdenes públicos", p. 9; MATELLANES RODRÍGUEZ, "Algunas notas sobre las formas de delincuencia informática en el Código Penal", pp. 142 y 143.

75 Lo señala GUTIÉRREZ FRANCÉS, "Delincuencia económica e informática en el nuevo Código Penal", pp. 297 y 298; ; también MATELLANES RODRÍGUEZ, "Algunas notas sobre las formas de delincuencia informática en el Código Penal", p. 142.

76 Véase ROVIRA DEL CANTO, *Delincuencia informática y fraudes informáticos*, pp. 236 y 237.

De aceptarse la exigencia de que el daño supere los cuatrocientos euros habría que tener en cuenta el menoscabo de la cosa, sea en su sustancia, sea en su funcionalidad[77], como se señalaba, sin considerar computables no obstante los costes de recuperación del sistema ni los efectos, por ejemplo, sobre la capacidad competitiva de la empresa, perjuicios a solventar en sede civil; tampoco el posible daño moral generado; ni, por supuesto, los costes generados para reparar las deficiencias de seguridad que han permitido el ataque al sistema[78].

Sea de una o de otra manera, está claro que, conforme a la ubicación del precepto y al concepto de patrimonio mantenido por doctrina y jurisprudencia, si el objeto afectado no tiene valor económico alguno, la conducta que afecte el mismo deberá considerarse atípica[79].

Parece adecuada, no obstante, una nueva regulación que tenga en cuenta la utilidad del dato para su titular, la importancia de la información afectada para su desenvolvimiento personal, el daño que se haya podido causar a su actividad. Piénsese en la Tesis doctoral borrada en todas sus copias por un virus[80]. Algo, sin embargo, de difícil admisión con la actual ubicación del precepto y su consideración eminentemente económica-patrimonial.

3. Tipo subjetivo

El artículo 264.2 exige una actuación dolosa. En supuestos como los de la introducción de virus en la Red que el autor desconoce si van a afectar efectivamente a algún usuario informático,

---

77 En contra, GONZÁLEZ RUS, "Daños a través de Internet y denegación de servicios", p. 1476; y MUÑOZ CONDE, *Derecho Penal. Parte especial*, pp. 474 y ss., rechazan que puedan tenerse en cuenta los daños derivados de la falta de funcionalidad del sistema afectado.

78 Véase FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet*, p. 117.

79 En este sentido, GONZÁLEZ RUS, "Daños a través de Internet y denegación de servicios", pp. 1476 y ss.

80 Contundentemente, CHOCLÁN MONTALVO, "Infracciones patrimoniales en los procesos de transferencia de datos", p. 93.

o a qué tipo de datos, programas o documentos va a hacerlo, no hay duda de que existe al menos dolo eventual, con lo que no se plantea ningún problema de subsunción a este respecto[81].

Puede suceder que los autores de la conducta típica pretendan un daño de una determinada gravedad que finalmente va más allá de lo previsto. Así, por ejemplo, con la introducción de un virus en un ordenador que se extiende, sin quererlo, a todos los ordenadores en contacto con el primero. Tampoco aquí debiera haber problemas para aceptar un dolo eventual, salvo en casos puntuales en que habría que recurrir a la imprudencia a tratar a través del art. 267, con las limitaciones de cuantía que en él se establecen. En ambos casos aplicando un concurso ideal de infracciones con los daños al primer ordenador generados con dolo directo[82].

Más problemático resulta el supuesto de introducción en un determinado programa de bombas lógicas que se activarán si se da una circunstancia determinada, como por ejemplo, que intente realizarse una copia del programa. En este caso, el autor no puede conocer si efectivamente se va a realizar el acto que desencadene la activación de la bomba lógica y hasta que este acto no se produzca, la introducción de la bomba lógica no podrá ser considerada sino un acto preparatorio impune. En cuanto se desencadene la activación de la bomba lógica la conducta podrá considerarse típica entendiendo que concurre dolo de dañar en el autor que la introdujo y no hizo nada para detener su activación[83].

No será necesario ningún elemento subjetivo del injusto adicional al dolo[84]; con independencia de que concurra o no, por

---

81 Véanse ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, p. 84.

82 Como afirman RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", p. 285.

83 Extensamente, ROMEO CASABONA, "Los delitos de daños en el ámbito informático", p. 108.

84 Expresamente FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet*, pp. 109 y 110; y ORTS BERENGUER/ROIG

ejemplo, un ánimo de lucro, que, en su caso, podría obligar a reconducir la tipificación —sólo en ocasiones— al ámbito de los fraudes informáticos[85].

Aunque el sujeto pasivo del delito no tuviese antivirus u otros medios de protección frente a ataques a su sistema y a los datos contenidos en él o no hubiera realizado copias de seguridad de sus documentos o programas, lo que podría denotar un comportamiento imprudente por su parte, la tipicidad de la conducta dañosa no ofrecerá duda alguna en esta sede. Esta ausencia de protección por parte del sujeto pasivo, de posible relevancia en sede civil, no puede suponer en ningún caso una circunstancia modificativa de la responsabilidad del autor que le exima de responsabilidad penal[86].

En cuanto a la causación de daños de modo imprudente, por ejemplo, a través de la distribución de archivos de procedencia dudosa, sin haber analizado previamente su peligrosidad, varios autores consideran desproporcionada o inadecuada la intervención penal en tales casos[87], considerando suficiente la reparación en sede civil[88]. Sin embargo, la posibilidad de apreciar el art. 267 está presente, siempre, claro está, que se cumplan los requisitos del mismo y, entre ellos, el de la causación de daños en cuantía superior a ochenta mil euros[89], a valorar también desde una

---

TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, p. 84.

85 Así, ROVIRA DEL CANTO, *Delincuencia informática y fraudes informáticos*, p. 226.

86 Expresamente MAGRO SERVET, "La responsabilidad civil y penal en el campo de la informática", p. 405.

87 Véanse las consideraciones de MORÓN LERMA, *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*, pp. 67 y 68.

88 Así, MATA Y MARTÍN, *Delincuencia informática y derecho penal*, p. 77.

89 En este sentido, GUTIÉRREZ FRANCÉS, "Delincuencia económica e informática en el nuevo Código Penal", p. 299. Destacan ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, p. 84, para quienes el artículo parece estar pensado para daños en elementos físicos, la dificultad de aplicación del precepto

perspectiva funcional, pero siempre en relación al perjuicio en el objeto, no a todo el derivado de la conducta típica.

4. Actos preparatorios, tentativa y consumación

El art. 6 del Convenio sobre Cibercriminalidad de Budapest exige sancionar las conductas de producción, venta, obtención, importación, difusión o simple posesión de dispositivos o palabras de paso que permitan la comisión de los delitos de daños informáticos. Aunque en un futuro también nuestro Código Penal incorpore la sanción de esta clase de actos preparatorios, obligatoria con la ratificación del Convenio, hasta la fecha no existe previsión alguna a este respecto.

En cuanto a la perfección del delito, de resultado, es factible la aparición de formas de ejecución imperfecta en que la consumación del delito no llega a producirse por causas ajenas a la voluntad del sujeto activo del mismo. Este supuesto es común, por ejemplo, en los casos en que se detecta por el usuario un virus que no llega a causar daño alguno o cuando teniendo potencialidad para causar un daño de grandes proporciones es detectado e inocuizado por un rastreo realizado por el antivirus habiendo producido un daño insignificante[90].

En los daños informáticos se plantean numerosos casos en los que transcurre un lapso de tiempo desde el inicio de la conducta hasta que se producen los resultados lesivos. A este respecto es discutible, por ejemplo, el momento en que se produce la consumación del delito en los supuestos de introducción de bombas lógicas, que es frecuente no se activen hasta pasados días, semanas e incluso meses o simplemente en los supuestos habituales de introducción de virus en la Red que no se sabe cuándo lograrán afectar a un sistema. Esta clase de supuestos ha de resolverse

justamente por la dificultad que supone computar el valor de los elementos dañados.

90 Así, ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, p. 85.

conforme a la Teoría general del delito como en cualquier otro caso. La consumación sólo se produce con el resultado previsto típicamente, que, en este caso, es el daño informático. Otra cosa es que el suceso que activa el virus o la bomba lógica sea incierto y el autor no sepa con certeza si se producirá o no, en cuyo caso la ejecución del delito no podrá entenderse iniciada hasta la producción de ese suceso[91]. Cuando el comienzo de la destrucción ya no pueda ser detenido por el autor o los daños se produzcan efectivamente habrá comenzado la ejecución del delito o consumado el mismo, respectivamente; y aunque se afirma que si el autor mantiene la posibilidad de paralizar los efectos destructores de la bomba lógica no puede entenderse comenzada la tentativa[92], ningún problema hay aquí también, mientras no se produzca un desistimiento voluntario, en entender estamos ya en el ámbito de ejecución delictiva.

Cuando se disponen de copias de seguridad de los datos, documentos o programas atacados algún autor niega que pueda afirmarse la consumación del delito, pues no hay permanencia del daño inicial producido[93], aceptando únicamente una tentativa punible[94] o, únicamente, una tentativa imposible[95]. La opción por la tentativa relativamente inidónea, punible, conforme a la explicación dogmática tradicional de ésta, parece la opción más viable. Ahora bien, una previsión legislativa, ajena a la estricta

---

91 Detenidamente, ROMEO CASABONA, "Los delitos de daños en el ámbito informático", pp. 109 y 110.

92 Así, CORCOY BIDASOLO, "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", pp. 1014 y 1015.

93 Véase GONZÁLEZ RUS, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", p. 7.

94 De esta opinión, entre otros, BUENO ARÚS, "El delito informático", p. 5; GONZÁLEZ RUS, "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes", p. 264; y ROMEO CASABONA, "Los delitos de daños en el ámbito informático", p. 110.

95 Así, MATA Y MARTÍN, *Delincuencia informática y derecho penal*, pp. 74 y ss., a no ser que el objeto del ataque vaya dirigido a destruir todas las copias existentes y no se consumado por razones ajenas a la voluntad del autor.

consideración económico-patrimonial de estas conductas y que tuviera en cuenta el hecho de la accesibilidad permanente a la información contenida en redes o sistemas informáticos podría permitir entender consumado el delito cuando, por ejemplo, se eliminan todos los datos de un fichero informático de especial trascendencia para el funcionamiento de una empresa del que existe una copia que no se encuentra en la sede física donde se han eliminado los datos o incluso cuando por la enorme cantidad de datos incluidos en ese fichero su reimplantación requiere varias horas o días, paralizándose toda una actividad profesional (o personal) durante este período de tiempo[96]. La tentativa, no obstante, seguiría siendo posible cuando la instalación de las copias fuera efectiva en un breve espacio de tiempo[97].

5. Penalidad, agravaciones y concursos

La pena señalada para el art. 264.2 es la misma que se establece para los daños del art. 263 cuando concurra alguna de las circunstancias del art. 264.1, penas de prisión de uno a tres años y multa de doce a veinticuatro meses. La cuestión, vinculada a la discusión sobre los requisitos de la tipicidad objetiva y la exigencia o no de que la cuantía del daño exceda de cuatrocientos euros, es si esta pena se aplica a todo tipo de daño informático doloso o si hay que acudir a la pena del art. 625 para cuando el daño no exceda esta cantidad, ya atendiendo el valor de mercado del objeto, ya su funcionalidad para su titular, opción, como se decía, no exenta de dificultades de aplicación, que incrementaría notablemente la aplicación de este último precepto.

Obviamente, las agravaciones del art. 264.1, y dado el tenor literal de éste, no son de aplicación, lo que no deja de suscitar

96 Extensamente, RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", pp.285 y 286.

97 Así, ROMEO CASABONA, "Los delitos de daños en el ámbito informático", p. 110. En contra, RODRÍGUEZ/LASCURAÍN/ALONSO, "Derecho Penal e Internet", pp. 285 y 286, opinan que es difícil que las copias de seguridad sean exactamente iguales a los originales dañados.

reservas[98]. Así, el delito de daños informáticos sería perfectamente compatible tanto con el primero de los supuestos recogidos en este precepto como con el último de ellos. El fundamento de agravación en ambos casos es independiente de la distinción entre daños comunes y daños informáticos. Obviamente, sería imposible la compatibilización de éstos con cualquiera de las otras tres circunstancias del precepto. Cierto es que no cabe la apreciación conjunta de dos o más de las agravantes del art. 264.1 y que en ese sentido puede también no ser indicada tampoco —por seguir el mismo criterio— la concurrencia de cualesquiera de ellas con la agravación que en sí ya implica el art. 264.2 respecto al art. 263, pero lo cierto es que el delito de daños informáticos es un tipo específico y así ha querido considerarlo el legislador con la ubicación que da al mismo.

Se plantea la duda de *lege ferenda* de si deben tratarse igual las conductas de destrucción o menoscabo definitivo de un programa, documento o dato que las de su inutilización o, más aún, alteración, sobre todo si se admite que éstas pueden tener carácter meramente temporal (lo que, no obstante, no parece viable con la actual ubicación)[99], lo que a nuestro juicio debiera depender del bien que se entienda protegido, del concepto que en general se mantenga del menoscabo patrimonial y de cuál sea la opción, mientras no se modifique la ubicación del precepto, que se tome en relación con menoscabos funcionales —incluso temporales— de un objeto cualquiera. En todo caso siempre queda el momento de individualización judicial de la pena para tener en cuenta posibles diferencias de desvalor de la conducta enjuiciada.

También se ha criticado que el art. 264.2 permita englobar conductas de consecuencias muy diferentes en cuanto a la gravedad del perjuicio causado[100]. Pero, de nuevo, la individualización

98 En este sentido, ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, p. 84.

99 Véase GARCÍA GARCÍA-CERVIÓN, "Daños informáticos. Consideraciones penales y criminológicas", p. 11.

100 Lo destaca CHOCLÁN MONTALVO, "Infracciones patrimoniales en los procesos de transferencia de datos", pp. 92 y 93.

judicial podrá tener en cuenta este hecho, al margen de la posibilidad concursal (de infracciones) que se ofrece siendo varios los titulares afectados.

En cuanto a esta posibilidad concursal, obviamente va a ser obligada también en numerosos supuestos, por ejemplo, en relación con la aplicación de los arts. 197 o 278.3.

Al concurso de normas habrá que acudir, en cambio, en los casos del art. 560.1, salvo que los daños causados fueran diversos y se lesionaran los bienes jurídicos, diferentes, de ambos preceptos[101].

V. Bibliografía

ÁLVAREZ VIZCAYA, M., "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red", en *Cuadernos de derecho judicial*, 2001, 10, 255-280.

ANARTE BORRALLO, E. "Incidencia de las nuevas tecnologías en el sistema penal", en *Derecho y conocimiento*, 1, 2001, 191-257.

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

BUENO ARÚS, F., "El delito informático", en *Actualidad Informática Aranzadi*, 11, 1994, 1-6.

CHOCLÁN MONTALVO, J.A., "Fraude informático y estafa por computación", en *Cuadernos de derecho judicial*, 2001, 10, 305-352.

CHOCLÁN MONTALVO, J. A., "Infracciones patrimoniales en los procesos de transferencia de datos", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 69-95.

CLIMENT BARBERÁ, J., "La justicia penal en internet. Territorialidad y competencias penales", en *Cuadernos de derecho judicial*, 2001, 10, 645-663.

101 Ampliamente MARCHENA GÓMEZ, "El sabotaje informático entre los delitos de daños y desordenes públicos", pp. 363 y ss.

CORCOY BIDASOLO, M., "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", en *La Ley*, 1, 1990, 1000-1016.

CORCOY BIDASOLO, M., "Problemas de la persecución penal de los denominados delitos informáticos", en *Eguzkilore*, 21, 2007, 7-33.

CRUZ DE PABLO, J.A., *Derecho Penal y Nuevas Tecnologías. Aspectos sustantivos*, Madrid, 2006.

DE ALFONSO LASO, D., "El hackering blanco. Una conducta ¿punible o impune?", en *Cuadernos de derecho judicial*, 2001, 10, 509-524.

DE LA MATA BARRANCO, N.J., *Tutela penal de la propiedad y delitos de apropiación*, Barcelona, 1994.

DE LA MATA BARRANCO, N.J., "Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general", en *Delito e informática: algunos aspectos*, Bilbao, 2007, 41-82.

ELOSUA, M./PLÁGARO, J., *Diccionario LID tecnologías de información y comunicación*, Madrid, 2007.

FERNÁNDEZ PALMA, R./MORALES GARCÍA, O., "El delito de daños informáticos y el caso Hispahack", en *La Ley*, 1, 2000, 1522-1529.

FERNÁNDEZ TERUELO, J.G., *Cibercrimen. Los delitos cometidos a través de Internet*. Oviedo, 2007.

GALÁN MUÑOZ, A., *El fraude y la estafa en los sistemas informáticos*, Valencia, 2005.

GALÁN MUÑOZ, A., "Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática", en *Revista de derecho y proceso penal*, 15, 2006, 13-38.

GALLARDO RUEDA, A., "Delincuencia informática: la nueva criminalidad de fin de siglo", en *Cuadernos de Política Criminal*, 65, 1998, 365-374.

GARCÍA GARCÍA-CERVIÓN, J., "Daños informáticos. Consideraciones penales y criminológicas", en *Actualidad Jurídica Aranzadi*, 588, 2003, 10-12.

GIMÉNEZ GARCÍA, J., "Delito e informática. Algunos aspectos de derecho penal material", en *Eguzkilore*, 20, 2006, 197-216.

GÓMEZ MARTÍN, V., "El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (art. 270, párr. 3º CP)", en *Revista electrónica de ciencia penal y criminología*, 4, 2002.

GONZÁLEZ RUS, J.J., "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", en *Revista de la Facultad de Derecho de la Universidad Complutense*, 12, 1986, 107-164.

GONZÁLEZ RUS, J. J., "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", en *Revista electrónica de ciencia penal y criminología*, 1, 1999.

GONZÁLEZ RUS, J.J., "Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (art. 264.2 Cp)", en *La Ciencia del Derecho penal ante el nuevo siglo. Homenaje al Profesor Dr. D. José Cerezo Mir*, Madrid, 2002, 1281-1298.

GONZÁLEZ RUS, J. J., "El Cracking y otros supuestos de sabotaje informático", en *Estudios Jurídicos del Ministerio Fiscal*, Madrid, 2003, 209-248.

GONZÁLEZ RUS, J. J., "Daños a través de Internet y denegación de servicios", en *Homenaje al Profesor Dr. Gonzalo Rodríguez Morullo*, Navarra, 2005, 1469-1488.

GONZÁLEZ RUS, J. J., "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 241-269.

GONZÁLEZ RUS, J. J., "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", en *Delito e informática: algunos aspectos*, Bilbao, 2007, 13-41.

GUTIÉRREZ FRANCÉS, M.L., *Fraude informático y estafa*, Madrid, 1991.

GUTIÉRREZ FRANCÉS, M.L., "Delincuencia económica e informática en el nuevo Código Penal", en *Cuadernos de derecho judicial*, 11, 1996, 247-306.

HUGHES, L.A./DE LONE, G.J. "Virus, Worms, and Trojan Horses. Serious Crimes, Nuisance or both?", en *Social Science Computer Review*, 25, 1, 2007, 78-98.

JORGE BARREIRO, A., "El delito de daños en el Código penal español", en *Anuario de derecho penal y ciencias penales*, 1983, 505-532.

LEZERTUA RODRÍGUEZ, M., "El proyecto de convenio sobre el cybercrimen del Consejo de Europa", en *Cuadernos de derecho judicial*, 2001, 10, 15-62.

LÓPEZ MORENO, J./FERNÁNDEZ GARCÍA, E.M., "La world wide web como vehículo de delincuencia: supuestos frecuentes", en *Cuadernos de derecho judicial*, 10, 2001, 399-456.

LÓPEZ ORTEGA, J.J., "Intimidad informática y derecho penal (la protección penal de la intimidad frente a las nuevas tecnologías de la información y comunicación)", en *Cuadernos de derecho judicial*, 2004, 9, 107-142.

MAGRO SERVET, V., "La responsabilidad civil y penal en el campo de la informática", en *Cuadernos de derecho judicial*, 7, 2003, 379-432.

MARCHENA GÓMEZ, M., "El sabotaje informático: entre los delitos de daños y desórdenes públicos", en *Cuadernos de derecho judicial*, 2001, 10, 353-366.

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

MATA Y MARTÍN, R.M., "Criminalidad informática: una introducción al cibercrimen (1)", en *Actualidad Penal*, 37, 2003, edición electrónica.

MATELLANES RODRÍGUEZ, N., "Algunas notas sobre las formas de delincuencia informática en el Código Penal", en *Hacia un derecho penal sin fronteras*, Madrid, 2000, 129-150.

MATELLANES RODRÍGUEZ, N., "Vías para la tipificación del acceso ilegal a los sistemas informáticos" en *Revista Penal*, 22, 2008, 50-68.

MORALES PRATS, F., "Internet: riesgos para la intimidad", en *Cuadernos de derecho judicial*, 10, 2001, 63-82.

MORANT VIDAL, J., *Protección penal de la intimidad frente a las nuevas tecnologías*, Valencia, 2003.

MORILLAS FERNÁNDEZ, D.L., *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comisivas relacionadas con Internet*, Madrid, 2005.

MORÓN LERMA, E., *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*, Cizur Menor (Navarra), 2ª ed., 2002.

MORÓN LERMA, E., "Derecho Penal y nuevas tecnologías: panorama actual y perspectivas futuras", en *Internet y pluralismo jurídico: formas emergentes de regulación*, Madrid, 2003, 93-120.

MUÑOZ CONDE, F., *Derecho Penal. Parte especial*, 16ª edición, Valencia, 2007.

ORTS BERENGUER, E./ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, Valencia, 2001.

PERARNAU MOYA, J., "Internet amenazada", en *Cuadernos de derecho judicial*, 10, 2001, 127-144.

QUINTERO OLIVARES, G., "Internet y propiedad intelectual", en *Cuadernos de derecho judicial*, 10, 2001, 367-398.

QUINTERO OLIVARES, G., *Comentarios a la Parte Especial del Derecho Penal*, 4ª edición, Cizur menor (Navarra), 2008.

RODRÍGUEZ MOURULLO, G./LASCURAÍN SÁNCHEZ, J. A./ALONSO GALLO, J., "Derecho Penal e Internet", en *Régimen jurídico de Internet*, Madrid, 2001, 257-310.

ROMEO CASABONA, C. M., *Poder informático y seguridad jurídica*, Madrid, 1988.

ROMEO CASABONA, C.M., "Los delitos de daños en el ámbito informático", en *Cuadernos de política criminal*, 43, 1991, 91-118.

ROMEO CASABONA, C.M., "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías", en *Poder Judicial*, 31, Madrid, 1993,163-204.

ROMEO CASABONA, C.M., "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet", en *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, 2, 2002, 123-149.

ROMEO CASABONA, C. M., "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 1-42.

ROMEO CASABONA, C.M., "Los datos de carácter personal como bienes jurídicos penalmente protegidos", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 167-190.

ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos*, Granada, 2002.

SÁNCHEZ GARCÍA DE PAZ, I. /BLANCO CORDERO, I., "Problemas de derecho penal internacional en la persecución de delitos cometidos a través de Internet", en *Actualidad Penal*, 7, 2002 (edición electrónica).

SERRANO GÓMEZ, A./SERRANO MAILLO, A., *Derecho penal. Parte especial*, Madrid, 2006.

SIEBER, U., "Criminalidad informática: Peligro y prevención" en *Delincuencia informática*, Barcelona, 1992, 13-47.

SIEBER, U., "Documentación para una aproximación al delito informático", en *Delincuencia informática*, Barcelona, 1992, 65-98.

VELASCO NÚÑEZ, E., "Aspectos procesales de la investigación y de la defensa en los delitos informáticos", en *La Ley*, 3, 2006 (edición electrónica).

VILLAMERIEL PRESENCIO, L.P., "Derecho Penal: algunas reformas necesarias en la actual legislatura" en *La Ley*, 6314, 2005 (edición electrónica).

WALL, D. S., "Cybercrime and the Culture of Fear. Social Science Fiction(s) and the Production of Knowledge about Cybercrime", en *Information, Communication & Society*, 11, 6, 2008, 861-864.

YAR, M., *Cybercrime and society*, London, 2006.