Daños informáticos

PID_00267793

Alfonso Galán Muñoz

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya

Alfonso Galán Muñoz

Profesor titular de Derecho penal de la Universidad Pablo de Olavide, doctor en Derecho y becario Formación de Profesorado Universitario (FPU) del Ministerio de Educación, de la Fundación Alexander von Humboldt y del Servicio Alemán de Intercambio Académico (DAAD). Ha realizado numerosas estancias de investigación en las universidades alemanas de Friburgo, Múnich, Tubinga y Berlín. Es experto en criminalidad informática y económica, temas a los que ha dedicado numerosas publicaciones, tanto nacionales como internacionales. Es investigador principal y miembro de varios proyectos de investigación nacionales y autonómicos, y responsable del Grupo PAIDI SEJ-571: Grupo de Investigación sobre el Sistema Penal y Criminología (SISPECRIM). También es el director del máster de Criminología y ciencias forenses de la Universidad Pablo de Olavide.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Josep Maria Tamarit Sumalla (2019)

Primera edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

La aparición y generalización del uso de sistemas informáticos llevó a que muchas entidades y particulares empezasen a utilizarlos para realizar y gestionar muchas de sus actividades profesionales y económicas, pero también muy diversos aspectos de sus vidas privadas, desde gestionar sus agendas a guardar los datos de sus amigos o conocidos o a archivar los vídeos y fotos de sus eventos personales y familiares.

Comenzó así una digitalización que no ha parado desde entonces. Esto llevó a que los datos y la funcionalidad de los sistemas informáticos que los contenían y procesaban fueran cobrando cada vez mayor importancia. No es solo que nos permitan conservar una cantidad cada vez mayor de informaciones referidas a nuestras vidas o documentos que resultan difícilmente reemplazables, sino que, además, tanto los datos como los sistemas informáticos de los que hablamos se han convertido en herramientas fundamentales para el desarrollo de las actividades de muchas empresas, e incluso del propio Estado.

Precisamente por ello, hace ya algún tiempo que el legislador tomó conciencia de la necesidad de que el derecho penal se utilizase para prevenir y castigar algunas de las conductas que tenderían a destruir, alterar o cuando menos inutilizar los sistemas informáticos y los datos que contienen, dados los muy nocivos efectos perjudiciales que dichas actuaciones podrían producir.

En concreto, se hacía necesario crear delitos que permitiesen castigar todas aquellas actuaciones perjudiciales que, por recaer en la parte lógica de los sistemas informáticos, y no en la física, no tendrían adecuado acomodo en la tradicional configuración de los delitos de daños, dado que, como es sabido, estas figuras exigen de la producción de una alteración en la sustancia de la cosa afectada por su realización para poder ser apreciados, lo que, evidentemente no se da cuando lo que se hace es simplemente alterar o borrar el registro electromagnético de un dato o un programa informático. Se dio así lugar a la creación de los delitos de daños informáticos, cuya concreta regulación ha ido evolucionando a lo largo de los años, hasta llegar a la que se contiene en nuestro Código penal tras su reforma por la LO 1/2015.

Mucho ha tenido que ver la Unión Europea (UE) en el devenir normativo de estas figuras. Es evidente que la clara proyección económica que presentan muchas de las conductas lesivas que castigan, unida a lo fácil y frecuente que resulta que generen efectos más allá del país donde se ejecutan (piénsese, por ejemplo, en los que produce la expansión de un virus en Internet), obligaron a la UE a dedicar una especial atención a armonizar la regulación penal creada para prevenir y sancionar su posible ejecución y efectos dentro de su territorio.

Así lo hizo, en primer lugar, mediante la Decisión Marco 2005/222/JAI del Consejo, que tanta influencia tuvo en la reforma penal referida a estos delitos que efectuó la LO 15/2010, como también y más recientemente lo ha hecho a través de la aprobación de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información (DAI), referente normativo que, como veremos, es básico a la hora de interpretar lo que nuestro Código penal establece con respecto a los daños informáticos tras la reforma que experimentó en 2015.

Objetivos

Después de trabajar los materiales que componen este módulo didáctico, el estudiante podrá alcanzar los siguientes objetivos:

1. Establecer qué clase de daños informáticos tendrán trascendencia penal y cuáles no.

2. Conocer las diferencias entre los delitos de daños por interferencia ilegal en datos informáticos y por interferencia en sistemas informáticos.

3. Distinguir los diferentes tipos cualificados aplicables a todos los delitos de daños informáticos.

4. Calificar adecuadamente conductas habituales de daños, como las de Ransomware o las que producen denegación de servicios.

5. Ser capaz de solventar los complejos problemas concursales que se plantean tanto entre las diferentes figuras de daños informáticos como entre estas y otros delitos del Código penal.

1. Bien jurídico protegido

La ubicación sistemática de los delitos de daños informáticos dentro del título XIII del libro II del Código penal, titulado «De los delitos contra el patrimonio y el orden socioeconómico», ya indica la clara naturaleza patrimonial o económica que tienen estas figuras (de otra opinión, sin embargo, por ejemplo, es Andrés Domínguez, 2016, quien, precisamente por ello, aboga por ubicar estas figuras, de *lege ferenda*, en un capítulo o sección independiente de aquella en la que está encuadrada hoy).

Esta consideración resulta fundamental para delimitar los injustos típicos de estos delitos, ya que, al no estar ante unas figuras que protejan el correcto funcionamiento de los sistemas informáticos o su seguridad, sino ante unos protectores del **patrimonio**, nunca y bajo ningún concepto se podrá apreciar su realización si la actuación llevada a cabo no llega a afectar, o cuando menos a poner en peligro, un valor de naturaleza patrimonial.

Estamos, por tanto, como señala Muñoz Conde (2017), ante unos delitos de daños patrimoniales, lo que, como veremos, debe tenerse muy en cuenta a la hora de delimitar e interpretar muchos de los elementos configuradores de sus tipos delictivos (por ejemplo, a la hora de definir quién puede excluir la tipicidad del borrado de unos datos mediante su consentimiento) y también al hacer lo propio con respecto a algunas de las circunstancias cuya concurrencia en su realización dará lugar a la apreciación de alguno de sus tipos cualificados (por ejemplo, el contemplado en el art. 264.2.2ª CP, que obliga a incrementar la pena atendiendo precisamente a la especial gravedad del daño ocasionado).

2. Los daños derivados de la interferencia ilegal en datos informáticos

2.1. Tipo básico

El artículo 264 CP establece que «El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años».

Este artículo trata de responder a lo exigido en el artículo 5 de la DAI, que obligaba a todos los Estados miembros a adoptar «las medidas necesarias para que borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad», mediante la introducción de una figura delictiva, cuyo injusto tiene varios elementos configuradores fundamentales que pasamos a analizar.

2.1.1. Tipo objetivo

Resulta indudable que nos encontramos ante una figura común que puede ser cometida por cualquier persona. No es necesario, por tanto, que su autor tenga ninguna posición especial con respecto a los datos que ataca y menos aún que tenga ninguna cualificación o preparación específica para poder ser responsabilizado por el mismo.

De forma plenamente concordante con lo anterior, este delito define su conducta típica de forma completamente abierta, señalando que podrá considerarse como tal cualquier actuación, realizada por cualquier medio, que pueda dar lugar a alguno de sus posibles resultados consumativos. Nos encontramos, por tanto, ante un delito puramente **resultativo**, y no de medios determinados, que permite castigar tanto al sujeto que utiliza sus especializados conocimientos informáticos para crear un complejo virus, o que bloquee o borre datos ajenos, como a aquel que los borra o inutiliza de una forma nada sofisticada (por ejemplo, magnetizando el soporte en que estaban almacenados).

Cualquiera de estas actuaciones, desde la más sofisticada hasta la más sencilla, tendrá cabida en este tipo delictivo. Sin embargo, para que la conducta de dicho sujeto pueda ser castigada conforme al mismo, se tiene que realizar **sin autorización y de manera grave**.

Lo primero nos obliga a tener que determinar quién será el sujeto que pueda dar la autorización que determinará que la actuación realizada sobre datos ajenos no tenga cabida en este tipo delictivo. Conforme a lo dispuesto en el artículo 2.d DAI, habría que entender que se considera que las interferencias de datos que castiga el vigente artículo 264 de nuestro Código penal se han efectuado «sin autorización» cuando no las haya autorizado «el propietario u otro titular del derecho sobre el sistema o parte del mismo» o si la ejecución no estuviera permitida «por el derecho nacional». Esta definición amplia, a nuestro modo de ver, parece estar mucho más orientada a delimitar quién puede autorizar los accesos ilícitos a sistemas informáticos de los que habla el artículo 3 DAI, y castiga nuestro vigente 197 bis.1 CP, que a definir quién puede hacerlo con las conductas dañinas de las que se ocupa el artículo 264 CP. Hay que perfilarla mucho más. Por ello, atendiendo a la naturaleza patrimonial que el legislador español ha dado a la figura aquí analizada, parece que lo más lógico es pensar que quien puede autorizar que se borre, destruya o inutilice un dato o un programa informático no es el titular del sistema físico en que estos se encuentran almacenados, como el precepto comunitario anteriormente comentado podría llevarnos a pensar, sino el propio titular del dato o programa afectado por dicho hecho, ya que es él, y solo él, quien es el titular del valor patrimonial afectado por la realización de este delito y, por tanto, el único legitimado para poder convertir en irrelevante su posible afectación. Así, por otra parte, lo demuestra el hecho de que el delito ahora analizado, como veremos, excluya de forma general la tipicidad de los daños realizados en datos o programas por su propio titular.

Por otro lado, la exigencia de que la conducta realizada haya de ser grave para poder tenerla por típica de este delito introduce un concepto jurídico indeterminado en la definición de su injusto que no se contemplaba en la DAI. Este concepto habrá de ser definido por nuestro tribunales, que serán quienes tengan que valorar la gravedad de la actuación lesiva realizada para poder incardinarla y castigarla por este delito (Castro Corredoira y Vázquez-Portomeñe Seijas, 2015), lo que, si bien no excluye que esta figura pueda castigar actuaciones no especializadas, pero sí dañinas para los datos o programas informáticos (por ejemplo, la destrucción de los datos mediante la destrucción física de su soporte), sí que llevará a que se tenga que dejar sin sanción aquellas que, pese a ocasionar daños graves, se realicen de una forma que no pueda considerarse como tal (por ejemplo, cuando se borran datos sin necesidad de vulnerar ninguna medida establecida para protegerlos y mediante el uso de un comando común que permite hacerlo en todos los sistemas).

Considerando 11 DAI

A este respecto, véase que el considerando 11 DAI, que autoriza a los Estados miembros a definir lo que se ha de entender en sus respectivos ordenamientos como casos de menor gravedad, alude solo a la gravedad de los resultados ocasionados y no a los medios para hacerlo.

No obstante, las referidas actuaciones no permitidas solo serán típicas de este delito en la medida en que ocasionen o tiendan a ocasionar un concreto resultado que determinará la consumación de esta figura.

En la medida en que dañen, deterioren, alteren, supriman o hagan inaccesibles datos, programas o documentos informáticos ajenos, cuando dicho resultado sea grave.

Tres son los elementos típicos básicos delimitadores de los posibles resultados consumativos de este delito. A saber:

1) Tiene que generarse un daño, un borrado, el deterioro, la alteración, la supresión o la inaccesibilidad de datos o programas informáticos.

2) Dicho efecto tiene que estar referido a programas o datos ajenos.

3) El resultado derivado del efecto producido sobre los datos o programas debe ser grave.

Lo primero establece una prolija y en ocasiones redundante enumeración de posibles resultados consumativos alternativos de este delito.

Esta enumeración permite apreciar este delito en su forma consumada, tanto si la conducta realizada elimina el programa o el dato en cuestión (**borrado o supresión**), lo cambia (**altera**), lo corrompe o inutiliza (**daña o deteriora**), como si, sin alterarlo ni suprimirlo, hace que su legítimo titular no pueda acceder a su contenido o no pueda utilizarlo (**lo hace inaccesible**), como sucede, por ejemplo, en los casos de uso del *Ransomware*, como el conocido *Wannacry*.

Ransomware

Ransomware es un software que restringe el acceso a partes o a todo el sistema informático ajeno, pidiendo generalmente a su titular un pago a cambio de devolvérselo, lo que determinará que, además de apreciarse el delito del que venimos hablando, se tenga que apreciar también el correspondiente delito de amenazas condicionales de mal constitutivo de delito (art. 169.1º CP).

La producción de uno cualquiera de estos resultados determinará la consumación del tipo objetivo de este delito.

Por otra parte, el hecho de que este delito solo permita castigar los daños que recaigan sobre **datos o programas ajenos** llevará a que, como ya hemos anticipado, queden al margen de su tipo de injusto los daños o alteraciones que realice sobre los mismos su propio titular. Esto pone de manifiesto el carácter eminentemente patrimonial de este delito, dado que, evidentemente, si un sujeto destruye sus propios datos, realiza un legítimo y, por tanto, atípico acto de disposición de su patrimonio que no puede tener relevancia penal.

Finalmente, el hecho de que el delito exija, para poder apreciar su realización, que el efecto ocasionado en los datos o programas ajenos deba ser considerado como **grave** obliga a tener que valorar la intensidad del efecto producido.

En tal sentido, Muñoz Conde (2017) señala, acertadamente a nuestro modo de ver, que la gravedad de cualquiera de estos resultados «debe referirse al valor patrimonial del objeto dañado o saboteado, dado que los daños tipificados en

este capítulo tienen que ser daños patrimoniales» y no al perjuicio patrimonial global finalmente producido con su realización, lo que le lleva a excluir de la valoración de dicha gravedad los daños morales o el lucro cesante producidos como consecuencia de su ejecución, perjuicios estos diferentes del daño propiamente dicho y que, a su juicio, solo podrán ser tenidos en cuenta a efectos de determinar la responsabilidad civil.

Mucho más discutible resulta, sin embargo, que a la hora de valorar la gravedad del resultado producido se tenga que tener en cuenta, como señala este autor, si la conducta realizada recayó sobre datos de los que se tenga una copia de seguridad o si su alteración podría ser solucionada mediante su reparación, ya que, además de que dicha postura parece hacer depender la valoración de la gravedad del daño ocasionado de la conducta autoprotectora de su víctima, protegiendo así más a quien menos se protege a sí mismo (por ejemplo, al que no hace copias de seguridad) y menos a quien sí lo hace, también llevaría a que algunos de los posibles resultados consumativos de este delito (por ejemplo, el bloqueo de datos o programas) quedasen prácticamente carentes de utilidad, dado su carácter generalmente reversible. Mucho más lógico resulta, a nuestro modo de ver, considerar que, a la hora de fijar si el resultado producido resulta grave o no, se deba atender, de forma análoga a lo que sucede con el resto de delitos de daños, exclusivamente al valor del daño producido al dato o programa en el momento en que se altera, suprime o bloquea, sin tener en cuenta, por tanto, la capacidad de autorreparación que tuviese su víctima, con lo que la posible reparación del daño ocasionado quedaría como una circunstancia cuya concurrencia solo podrá ser tenida en cuenta, a efectos penales, cuando hubiese sido realizada por el responsable del delito y no por su víctima, y concurriendo el resto de requisitos que permitirían apreciar la atenuación que establece el artículo 21.5ª CP.

Finalmente, con respecto a la valoración de la gravedad del resultado típico de este delito, cabe señalar que el hecho de que el legislador haya optado por no utilizar una cuantía objetiva a la hora de delimitar tal resultado, como ha hecho, por ejemplo, en el tipo tradicional de daños del artículo 263 CP, es claro indicativo, a nuestro modo de ver, de que el límite cuantitativo contemplado en este último delito y en otros patrimoniales con la intención de diferenciar sus tipos básicos de los delitos leves que también contemplan (superar o no los 400 €), no debe emplearse a la hora de juzgar la gravedad del resultado que exige el delito de daños informáticos aquí analizado para poder ser apreciado. Así lo demuestra, a nuestro juicio, el hecho de que dicha omisión manifieste la tácita voluntad legislativa de no aplicar tal límite cuantitativo al delito que estamos analizando, pero también, y especialmente, que nuestro legislador haya decidido no establecer un delito leve para sus casos menos graves, como sí hizo en los delitos patrimoniales, lo que llevará a que cualquier ataque informático de los que venimos hablando que no alcance la gravedad exigida por este delito quede en la más absoluta atipicidad.

Debe tenerse en cuenta, en tal sentido, que el artículo 5 DAI obliga expresamente a que todos los Estados miembros deban castigar penalmente los ataques aquí contemplados «al menos en los casos en que no sean de menor gravedad», lo que conforme afirma el considerando 11 de dicha Directiva, solo les permitirá dejar sin sanción penal aquella interferencia sobre datos o programas informáticos que, atendiendo al «daño causado por la infracción o el riesgo que acarree para intereses públicos o privados, como la integridad de un sistema o datos informáticos, la integridad, derechos u otros intereses de una persona, resulte insignificante o sea de una índole tal que no resulte necesario imponer una pena dentro del umbral jurídico ni exigir responsabilidad penal».

Así, pues, tanto el legislador como los jueces españoles (no olvidemos que estos últimos tienen que hacer una interpretación integradora de las normas nacionales conforme a lo dispuesto en las europeas –STEJ Pupino–) tendrán que castigar las conductas aquí analizadas mientras no ocasionen un daño que se pueda considerar como insignificante, algo que, evidentemente, no se da en todos los daños menores o iguales a 400 €, dado que si la generación de daños de dicha cuantía es considerada como suficiente para poder ser castigada como leve en otros delitos, no puede tenerse por insignificante con respecto al aquí estudiado, lo que obliga a castigar su producción por el mismo.

2.1.2. Tipo subjetivo

El artículo 264 CP castiga la realización dolosa de su injusto típico, lo que, unido al carácter de delito de resultado-lesión que presenta su configuración típica, abre las puertas a que se pueda castigar su imperfecta ejecución mediante la apreciación de su tentativa. Por otra parte, su carácter doloso también determina que cualquier error referido a cualquiera de los elementos delimitadores de su tipo objetivo (por ejemplo, la ajenidad del dato afectado o la presencia del consentimiento de su titular) excluya la aplicación de la pena contenida en dicho delito.

No obstante, el hecho de que esta figura se haya configurado inicialmente de forma dolosa, lo que se ajusta perfectamente a lo establecido en la DAI, que solo obliga a los países miembros de la UE a castigar las interferencias ilegales en los datos de las que habla su artículo 5 cuando se realicen «intencionadamente», no impide que nos tengamos que plantear si también cabría sancionar su realización imprudente, atendiendo al hecho de que el artículo 267 de nuestro Código penal establece que «Los daños causados por imprudencia grave en cuantía superior a 80.000 euros serán castigados con la pena de multa de tres a nueve meses, atendiendo a la importancia de los mismos».

El problema que se plantea entonces es el de determinar si esta clausula sancionadora de la comisión imprudente de los delitos de daños resulta predicable o no con respecto al delito de daños informáticos que venimos analizando.

En tal sentido, resulta evidente que el hecho de que la DAI solo obligue a castigar las conductas aquí analizadas cuando se realizan de forma dolosa, no impide, ni puede impedir, que el legislador español pudiese decidirse a castigar también las imprudentes. La DAI solo impone un mínimo sancionador a los Estados miembros con respecto a las conductas que contempla, que los legisladores nacionales han de alcanzar, pero que evidentemente, como lamentablemente demuestran muchos artículos de nuestro Código penal, pueden superar si quieren.

Precisamente por ello, y teniendo en cuenta que cuando el legislador de 2015 pretendió excluir la aplicación de algunas de las prescripciones generalmente previstas para los daños con respecto a los daños informáticos, manifestó expresamente dicha voluntad (véase, por ejemplo, que el art. 266 CP limita su aplicación a los delitos del art. 263 CP y no a los aquí analizados), algo que, sin embargo, no hizo en el artículo 267 CP, consideramos que no quedará más remedio que entender que la previsión referida al castigo de la imprudencia establecida en este último precepto resulta plenamente aplicable a todos los delitos contenidos en el capítulo de daños, entre ellos los daños informáticos. Habrá que entender, entonces, que cuando los daños sobre datos o programas informáticos de los que venimos hablando se ocasionen por imprudente grave (por ejemplo, por haber cometido un error técnico que ocasione la pérdida no deseada de datos o por haber errado sobre el carácter ajeno de los borrados o con respecto a la autorización para hacerlo), se podrá castigar a quien los haya generado, atendiendo a lo dispuesto en el artículo 267 CP, siempre y cuando, eso sí, su conducta dé lugar a un daño que, tal y como exige dicho precepto, supere los 80.000 € y el agraviado o, en determinados casos, el Ministerio Fiscal haya solicitado su persecución.

2.2. Tipos cualificados

El artículo 264 de nuestro Código penal contempla toda una serie de tipos cualificados aplicables a la modalidad básica de dicho delito, esto es, a aquella que castiga los daños dolosos por interferencia en los datos que, como acabamos de ver, contempla y sanciona el primer apartado del referido artículo.

Veamos dichos tipos someramente.

1) Por su comisión en el marco de una organización criminal

El primero de estos posibles tipos está recogido en el artículo 264.2.1º CP, que obliga a castigar con una pena de prisión de hasta cinco años la comisión del delito de daños por interferencia en los datos que se hubiese **cometido en el marco de una organización criminal**.

Nuestro ordenamiento responde así a lo exigido por el artículo 9.4.a DAI, que obligaba a los Estados miembros a castigar la comisión de este tipo de delitos con una pena máxima de al menos cinco años si se cometen en el contexto de una organización delictiva de las que habla la Decisión Marco 2008/841/JAI.

Parece que lo que pretende la creación de este tipo cualificado es responder a la aparición de grupos de piratas informáticos, altamente especializados en la realización de este tipo de actividades y que incluso se ofrecen a terceros para llevarlas a cabo a cambio de una determinada remuneración (Quintero Olivares, 2016).

Sin embargo, lo único que este tipo necesita para poder ser apreciado es que el delito de daños sobre datos realizado se cometa en el marco de una organización criminal. Esto es, en el seno de una organización que esté destinada a cometer delitos en general, tal y como establece el artículo 1.1 de la citada Decisión Marco 2008/841/JAI y el artículo 570 bis.1 de nuestro Código penal, y no de una que haya de estar exclusiva o primordialmente dirigida a cometer delitos de daños informáticos. Por un lado, esto permitirá, evidentemente, que esta cualificación se pueda aplicar al delito de daños cometido en tales organizaciones de forma puramente puntual u ocasional y, por otro, también determinará que la apreciación de esta cualificación resulte absolutamente incompatible con la de cualquiera de los delitos de pertenencia a dicho tipo de organizaciones que castigan los artículos 570 bis y siguientes de nuestro Código penal, con los que la cualificación aquí analizada –no el delito del tipo básico de daños sobre datos que siempre se habrá de apreciar– entrará en concurso de leyes.

2) Por producir daños de especial gravedad o por afectar a un número elevado de sistemas informáticos

El segundo apartado del artículo 264.2 CP obliga a imponer una pena de hasta cinco años de prisión a aquellos casos en los que los daños ocasionados sean de especial gravedad o bien se haya afectado a un número elevado de sistemas informáticos.

Lo primero, que responde a lo exigido en el artículo 9.4.b DAI, atiende al daño, no al perjuicio, lo que lleva a que tampoco aquí se puedan tener en cuenta ni valorar los lucros cesantes o los perjuicios morales derivados de la conducta de daños efectuada. Teniendo en cuenta que estamos, como ya hemos visto,

ante un delito eminentemente patrimonial y que existen otras muchas figuras de dicha naturaleza que incrementan su pena atendiendo a la gravedad del daño o perjuicio que producen, fijada en si superan los 50.000 € para considerarlos como especialmente graves, creemos que lo más adecuado es fijar también dicha cuantía como referente del daño que permitirá apreciar este tipo cualificado.

La segunda de las posibles circunstancias cualificadoras contemplada en el artículo 264.2.b CP responde a lo exigido por el artículo 9.3 DAI, que obliga a incrementar la pena de los ataques informáticos aquí analizados que afecten a «**un número significativo de sistemas de información**». De hecho, el precepto español responde con creces a lo exigido por este precepto comunitario, ya que mientras este solo exigía que dichas conductas se castigasen con una pena máxima no menor a los tres años de prisión, el artículo español permite, como ya hemos señalado, que se puedan castigar con hasta cinco años de privación de libertad.

Tal vez por eso nuestro texto legal exige que se afecte a un «**número elevado de sistemas informáticos**» y no simplemente a uno «significativo» como hace la DAI, lo que, a nuestro modo de ver, debería llevarnos a limitar la aplicación del tipo cualificado a aquellos casos en los que el número de sistemas afectados sea enorme y no simplemente significativo. Es decir, que hablemos de miles de sistemas afectados y no solo de unos cientos. En cualquier caso, resulta reseñable que este tipo atienda al número de sistemas afectados, esto es, de aparatos o grupos de aparatos interconectados que realizan un tratamiento automatizado de datos (art. 2 DAI) y no al número de personas que sufriesen el ataque, lo que permitirá que se pueda apreciar esta cualificación cuando se afecte a un número elevado de ordenadores o redes de una sola persona o entidad (por ejemplo, una gran empresa o una administración), por más que, de hecho, solo se perjudique el patrimonio de un único sujeto pasivo.

3) Por perjudicar gravemente servicios públicos esenciales o la provisión de bienes de primera necesidad

La cualificación contemplada en el tercer apartado del artículo 264.2 CP permite que se pueda elevar la pena del autor de estos delitos hasta los cinco años en los casos en que su conducta perjudique gravemente el funcionamiento de servicios públicos esenciales o lo haga con la provisión de bienes de primera necesidad.

Como señala Benítez Ortúzar (2015), este tipo requeriría de la realización de unos daños que habrán de presentar una triple gravedad para poder permitir su apreciación. Tendrán que ser unos daños cometidos mediante una actuación

que se considere como grave, que afecten de dicha forma a los datos informáticos sobre los que recaigan y que, además, perjudiquen también gravemente servicios públicos esenciales o la provisión de bienes de primera necesidad.

Evidentemente, este último resultado grave no es un resultado puramente informático, sino que alude a un efecto derivado de la supresión o la alteración de datos realizada. Es decir, se podrá apreciar este tipo si el borrado o la inutilización de un programa dolosamente producida, determina que no se pueda prestar o se haga con extrema dificultad (recuérdese que la afectación debe ser grave) algún servicio público esencial, como podrían ser, por ejemplo, el sanitario, el relativo al trasporte ferroviario o aéreo o si se ocasiona dicho efecto respecto a la provisión de bienes de primera necesidad, esto es, aquellos productos que resultan esenciales para la vida o la salud de las personas (alimentos, medicamentos, electricidad, agua, etc.).

En cualquier caso, cabe reseñar que si el perjuicio al servicio público o a la provisión de bienes de primera necesidad se derivase de la paralización o ralentización del sistema informático atacado, y no simplemente de la pérdida o bloqueo de algún dato o programa, habrá de apreciarse el tipo cualificado del delito de interferencia en sistemas informáticos del artículo 264 bis.2 CP y no el aquí comentado, atendiendo, tal y como veremos, tanto a la mayor especialidad que presenta dicho precepto respecto a este caso como a su mayor pena.

Como se puede comprobar, el fundamento de este tipo cualificado es claramente social y supraindividual, y no puramente patrimonial, lo que en algunas ocasiones va a determinar que se solape con el que vamos a analizar a continuación, referido a los ataques realizados contra los denominados sistemas de información de una infraestructura crítica.

4) Por afectar a algún sistema de información de una infraestructura crítica o creación de una situación de peligro grave para la seguridad del Estado, de la UE o de algún Estado miembro

El origen de la cualificación referida a la afectación de sistemas informáticos de una infraestructura crítica que contempla nuestro artículo 264.2.4º CP se encuentra, de nuevo, en la tantas veces citada DAI.

> Fue en el considerando 4 de dicha norma comunitaria donde expresamente se afirmó que «Existe en la Unión una serie de infraestructuras críticas cuya perturbación o destrucción tendría repercusiones transfronterizas importantes. De la necesidad de incrementar en la Unión la capacidad de protección de estas infraestructuras se desprende que las medidas contra los ataques informáticos deben complementarse con penas estrictas que reflejen la gravedad de tales ataques».

Precisamente por ello, el artículo 9.4 DAI obliga a los Estados miembros de la UE a incrementar la pena aplicable a los daños informáticos anteriormente comentados si se cometen contra el sistema de información (lo que, conforme al art. 2.a DAI, incluye datos, programas y el propio sistema en sí) de una infraestructura crítica, mandato que ha sido cumplido por España mediante la creación del tipo cualificado contemplado en el vigente artículo 264.2.4º CP.

Lo primero que habría que definir es qué habrá de considerarse por una de las infraestructuras críticas cuyos datos y programas protege el tipo cualificado ahora analizado. Dicho concepto ha sido definido expresamente por el propio legislador penal, al establecer en el artículo 264.2.4º CP que «A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población, como las centrales eléctricas, las redes de transporte y las redes de los órganos de gobierno, y cuya perturbación o destrucción tendría un impacto significativo en un Estado miembro al no poder mantener esas funciones».

Esta definición, que es plenamente coincidente con la contenida en el ya citado considerando 4 de la DAI y también con la del artículo 2.a de la Directiva 2008/114/CE, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, fue desarrollada a nivel nacional mediante la aprobación de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Precisamente, ha sido en esta ley, en concreto en su artículo 4, donde se ha establecido la obligación del Ministerio del Interior de crear un catálogo nacional de infraestructuras críticas, en el que se incluirán todas aquellas que cumplan con los requisitos que su reglamento de desarrollo establezca para poder ser clasificadas como tales.

Con respecto a los sistemas españoles, habrá que acudir, por tanto, a tal catálogo, que debería contener siempre información completa actualizada e informatizada relativa a tales infraestructuras (véase art. 2.o de la Ley 8/2011), para determinar si el ataque realizado sobre los mismos podría ser castigado o no conforme a lo establecido en el tipo cualificado que venimos analizando, aunque evidentemente si alguna de las infraestructuras incluidas en dicho catálogo no cumpliese con los requisitos que establece la Ley 8/2011 o su Reglamento de desarrollo, especialmente el artículo 264.2.4º CP, para poder considerarlas como tales, debería entenderse que la referencia a la misma sería nula, impidiéndose así que el ataque realizado contra los datos o programas de sus ordenadores pudiese ser castigado mediante la apreciación de este tipo cualificado.

Ahora bien, pese a lo amplio que puede resultar este catálogo, en el que, como acabamos de ver, se incluyen expresamente los sistemas esenciales para el mantenimiento de la seguridad y cuya afectación daría lugar a la cualificación

aquí comentada, el legislador ha decido castigar también cualificadamente en este precepto aquellos daños sobre datos que **creen una situación de peligro grave para la seguridad del Estado, de la UE o de un Estado miembro**. Lo importante aquí no es que se afecte a un sistema crítico para la seguridad nacional, sino que el ataque realizado a un sistema, incluso aunque no tuviese dicha consideración, genere un peligro grave para alguno de dichos valores. Es decir, que se ocasione un resultado de peligro real y efectivo para tales intereses, un peligro concreto.

Como señala Quintero Olivares (2016), la propia imprecisión del concepto de seguridad del Estado y el hecho de que en muchos casos se haya utilizado su supuesta protección para justificar muchos abusos graves cometidos por los Estados deben llevarnos a actuar con cautela a la hora de aplicar esta cualificación, por lo que la misma debe ser objeto de una interpretación claramente restrictiva que debería llevarnos a que solo se pueda apreciar su concurrencia en los daños informáticos ocasionados al margen de los sistemas calificados como críticos para la seguridad nacional, cuando la situación de riesgo ocasionada para tal seguridad sea tan grave y manifiesta que no se pueda discutir su existencia.

5) Por haber utilizado alguno de los medios a que se refiere el artículo 264 ter CP

El legislador español ha decidido castigar con una pena que puede llegar hasta los cinco años de prisión al sujeto que hubiese cometido el delito de daños del que venimos hablando si se utiliza alguno de los medios a los que se refiere el artículo 264 ter CP. Esto es, alguno de los programas informáticos concebidos o adaptados principalmente para cometer estos delitos o de las claves o de las contraseñas que permitan acceder a todo o a parte de un sistema de información de los que habla dicho artículo, instrumentos todos ellos que analizaremos con mayor detalle al analizar el referido precepto.

Ved también

Análisis detallado en el apartado «La producción, adquisición o facilitación de instrumentos dirigidos a cometer daños informáticos» del presente módulo.

De nuevo nos encontramos con una cualificación que responde con creces a una exigencia comunitaria. En concreto, a aquella que establece el artículo 9.3 DAI y que obliga a castigar los delitos de daños informáticos cometidos con tales instrumentos con una pena cuyo máximo debería ser de al menos tres años.

Evidentemente, la apreciación de este tipo cualificado determinará que no pueda castigarse a su autor por el delito que sanciona los actos referidos a la mera producción, tenencia o distribución de las referidas herramientas efectuadas para cometerlo, por cuanto, al castigar esta última figura meros actos

preparatorios del uso de los medios que precisamente castiga el tipo cualificado aquí analizado, habrá que entender que la apreciación de este último tipo absorberá el completo desvalor del injusto que castiga aquel.

Por otra parte, algo parecido sucederá con respecto al delito de acceso ilegítimo a sistemas informáticos que castiga el artículo 197 bis.1 CP y con el delito de creación o suministro de claves que castiga el 197 ter.a CP, dado que, al castigar el tipo cualificado aquí analizado, entre otros, precisamente los daños a datos o programas que se hubiesen realizado mediante el uso de las claves que permiten entrar a ordenadores ajenos, cuando ello suceda y se dañen datos accediendo indebidamente a los sistemas que los contienen gracias a dichas claves, los injustos derivados del acceso ilícito realizado (art. 197 bis.1 CP), así como el propio de la creación o suministro de las códigos utilizados para hacerlo (art. 197 ter.a CP), quedarán completamente absorbidos y valorados por la figura aquí analizada, sin que, consecuentemente, se pueda volver castigar a su autor por haberlo hecho mediante la simultánea apreciación de ninguna de las referidas figuras protectoras de la intimidad y la inviolabilidad informática.

6) Por la extrema gravedad del hecho realizado

El último inciso del artículo 264.2 CP determina que si los daños realizados sobre datos o programas informáticos se considerasen como de extrema gravedad, se imponga a su autor la pena prevista para los tipos cualificados de dicho precepto en su mitad superior. Nos encontramos ante una clausula ciertamente abierta, que define un tipo supracualificado de esta figura. Curiosamente, este tipo, a diferencia de muchos de los anteriores, no tiene origen en ninguna prescripción de la DAI, con lo que ninguna de las prescripciones de la citada norma comunitaria puede orientarnos respecto a su interpretación y delimitación.

A nuestro modo de ver, lo más adecuado para dotar de cierta seguridad jurídica a este precepto será entender que el mismo podrá apreciarse:

a) Cuando una de las circunstancias que determinan la apreciación del tipo cualificado del artículo 264.2 CP se dé de forma **especialmente intensa** (por ejemplo, se ocasionen daños que superen con creces los 50.000 € que delimitarán los de especial gravedad, como serán los superiores a los 250.000 €).

b) Cuando **concurra simultáneamente más de una de las circunstancias determinantes de los tipos cualificados precedentes** (por ejemplo, cuando se ocasione un daño que afecte a un número elevado de sistemas y además perjudique gravemente el funcionamiento de un servicio público esencial o se realice dentro de una organización criminal y ocasionando daños de especial gravedad).

7) Por haberse realizado mediante el uso de datos personales ajenos

El artículo 264.3 CP, en respuesta a lo exigido en el artículo 9.5 DAI, establece una nueva cualificación que incrementará la pena aplicable a los responsables de los delitos de daños de los que venimos hablando en aquellos casos en que los hubiesen realizado mediante la utilización de datos personales ajenos para facilitar el acceso al sistema informático o ganarse la confianza de un tercero.

Este precepto tiene por finalidad reprimir de forma más severa todos los daños sobre datos y programas que se realizan mediante la previa comisión de una de las muchas formas de posible realización de lo que se ha dado en llamar «**robo o usurpación de identidad**». Precisamente por ello, el incremento de penas previsto en el artículo ahora comentado resulta predicable tanto con respecto al delito de tipo básico del artículo 264.1 CP como en relación con cualquiera de los tipos cualificados que se contemplan en el apartado 2 de dicho artículo, lo que da lugar, en este último caso, a la apreciación de una supracualificación.

Lectura recomendada

Sobre el robo o usurpación de identidad, véase **A. Galán Muñoz** (2010). «El robo de identidad: aproximación a una nueva y difusa conducta delictiva». En: A. Rallo Lombarte; L. Arroyo Zapatero; I. Alamillo Domingo, y otros. *Robo de identidad y protección de datos* (págs. 169-198). Cizur Menor: Aranzadi.

No obstante, son varios los preceptos de nuestro Código penal que permitirían castigar algunos de estos usos de datos ajenos, lo que planteará diversos problemas concursales.

En primer lugar, si el dato personal ajeno utilizado para efectuar un daño sobre datos o programas informáticos ajenos es precisamente aquel que sirve de clave de acceso al sistema que los contiene (piénsese, por ejemplo, en los datos biométricos del titular del sistema usados para proteger el acceso al mismo), la conducta realizada mediante su uso podría ser castigada tanto a través de la apreciación de este tipo cualificado, como con la del contemplado en el artículo 264.2.5º CP, aunque sin que los dos tipos se puedan aplicar de forma simultánea, por lo que ambos entrarían en un concurso de leyes que habrá de resolverse atendiendo al **principio de alternatividad**.

En otro orden de cosas, es evidente que la ejecución del tipo cualificado aquí comentado siempre supone una utilización no autorizada de datos personales ajenos en perjuicio de un tercero, lo que, en determinadas ocasiones, como analizamos en otro lugar de esta asignatura, también podrá ser castigado por el delito del artículo 197.2 CP, con el que la cualificación aquí comentada (no el tipo básico de daños, que sí que resulta compatible con el delito del artículo 197.2 CP) también entrará en concurso de leyes con tal delito, concurso que habrá de solventarse por alternatividad.

Finalmente, solo resta por señalar que la **suplantación de identidad** que contempla el tipo cualificado del delito de daños del que venimos hablando puede ser puramente temporal u ocasional, con lo que la apreciación de esta cualificación no siempre y necesariamente supondrá la comisión del delito de

usurpación de estado civil del artículo 401 CP. Este último delito, como es sabido, requiere una continuidad en el uso de la identidad ajena para poder ser apreciado, por lo que su efectiva realización sí que supone y, por tanto, absorbe la suplantación puntual de identidad que define el tipo cualificado ahora comentado. Por ello, en caso de que se pueda apreciar la efectiva realización del delito de usurpación de estado civil en la comisión de un delito de daños informático, el castigo de dicho delito resultará incompatible con el del tipo cualificado de daños informáticos del que venimos hablando, existiendo, por tanto, un concurso de leyes entre el delito del artículo 401 CP y esta cualificación (no con el tipo básico de daños, que es compatible con el delito del art. 401 CP, con lo que podrá y, en su caso deberá, entrar en concurso de delitos con él), que habrá de resolverse aplicando aquella calificación típica que determine la aplicación de la pena mayor.

3. Los daños derivados de la interferencia ilegal en sistemas de información

3.1. Tipo básico

El artículo 264 bis CP castiga con pena de prisión de seis meses a tres años al «que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:

1) realizando alguna de las conductas a que se refiere el artículo 264 bis CP;

2) introduciendo o transmitiendo datos; o

3) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica».

Se introduce así en nuestro ordenamiento, supuestamente en respuesta a lo exigido por el artículo 4 DAI, una figura que, como veremos, es mucho más amplia que la que dicha norma comunitaria realmente obligaba a crear. Analicemos su tipo de injusto.

3.1.1. Tipo objetivo

El delito de daños por interferencia ilegal en los sistemas de información contemplado en el artículo 264 bis CP castiga la producción de dos posibles resultados alternativos, pero solo lo hace si tales resultados se producen mediante la realización de alguna de las conductas que su tipo de injusto enumera y describe también de forma alternativa, lo que indudablemente convierte a esta figura en un delito de medios determinados y no puramente resultativo.

En concreto, este delito se puede cometer mediante alguna de las siguientes conductas:

1) Realizar alguna de las actuaciones contempladas en el delito de daños en datos o programas informáticos del artículo 264 CP que ya analizamos. Esto es, **suprimir, borrar, dañar o hacer inaccesibles sin autorización y de forma grave datos o programas informáticos**, lo que, evidentemente, supone que si el delito de daños sobre sistemas aquí analizado se comete mediante esta modalidad comisiva, su apreciación absorberá el injusto de la figura contenida en el artículo 264 CP.

2) Introducir o transmitir datos. Estas conductas pueden llegar a producir alguno de los resultados típicos de este delito, tanto saturando la memoria o el disco duro del ordenador (piénsese, por ejemplo, en el virus informático que se reproduce hasta saturar el sistema en el que se implanta) como haciendo que un sistema conectado a una red reciba un bombardeo tal de peticiones de servicio desde diferentes ordenadores (en muchas ocasiones integrados en *botnets* sin conocimiento de sus titulares) que terminen por saturar el sistema y bloquearlo, o cerrar el acceso a la red de que dispone, impidiendo de esa forma que otros usuarios pudiesen utilizarlo (los ataques de *Distributed Denial of Service* o *DdoS*).

2) Destruir, dañar, inutilizar, eliminar o sustituir un sistema informático, telemático o de almacenamiento de información. Esta novedosa modalidad comisiva, que no estaba contemplada en la figura que precedió a la ahora analizada antes de la reforma de 2015, tampoco aparecía contemplada ni exigida en el artículo 4 DAI. Es, por tanto, una modalidad o creación puramente nacional que parece que lo que pretende es que la figura ahora penada permita castigar las interferencias en el funcionamiento de los sistemas informáticos que se realicen dañando o manipulando su hardware. Es decir, sus componentes físicos y no meramente digitales, lo que nos lleva a entender que si el delito aquí analizado se cometiese, por ejemplo, mediante la destrucción o el deterioro físico de tales sistemas, su apreciación absorbería el concreto delito de daños del artículo 263 CP que valorase y castigase el concreto daño físico que se les hubiese ocasionado.

Cualquiera de estas actuaciones podrá dar lugar al delito que venimos analizando siempre y cuando, eso sí, resulte adecuada y se efectúe con la intención de producir alguno de los resultados que determinarían su consumación delictiva.

Los resultados, como ya hemos señalado, pueden ser dos. O bien se **interrumpe** el funcionamiento de un sistema informático ajeno, es decir, se bloquea e impide que funcione, o bien se **obstaculiza**, lo que simplemente supone que el sistema funcione más lentamente o de forma menos eficaz a como lo haría antes de la realización de la conducta en cuestión.

> Sin embargo, para que cualquiera de dichos resultados dé lugar a la apreciación de este delito, se requerirá que se hayan ocasionado sin estar autorizado y de manera grave.

Lo primero determina que solo entren en este tipo delictivo las conductas obstaculizadoras o interruptoras del funcionamiento del sistema informático que se realicen **sin autorización**, algo que, atendiendo a lo que establece el ya anteriormente citado artículo 2.d DAI, determinará que queden al margen de este tipo delictivo tanto aquellas actuaciones que estén autorizadas por el

derecho nacional (por ejemplo, el bloqueo del acceso a un servidor en cumplimiento de una resolución judicial en tal sentido) como las que se hayan llevado a cabo con el consentimiento del titular del sistema afectado o con el de quien, por lo menos, tenga un derecho de uso sobre el sistema o una parte del mismo (por ejemplo, quien había alquilado el sistema o una parte del mismo para tratar, almacenar o comunicar sus datos).

Por su parte, el hecho de que las interrupciones u obstaculizaciones de los sistemas no puedan dar lugar a este delito a no ser se las pueda tener por **graves** nos lleva a pensar, atendiendo al carácter netamente patrimonial que presenta este delito, que solo podrán ser castigadas conforme al mismo las interferencias en sistemas informáticos que afecten severamente a dicho bien jurídico protegido. Esto es, al patrimonio.

No podrán castigarse, entonces, por esta figura la paralización o ralentización de sistemas que carezcan de trascendencia económica (por ejemplo, la del ordenador que se utilice a efectos meramente lúdicos), sino tan solo la de aquellos equipos cuyo uso, interrumpido o ralentizado por la actuación efectuada, tenga efectos económicos o patrimoniales por determinar la aparición de un perjuicio patrimonial. Este resultado, al tener que producirse en este delito como consecuencia de la alteración del funcionamiento del sistema producido, generalmente vendrá dado por el lucro cesante que el anormal funcionamiento del sistema ocasionaría (por ejemplo, de las pérdidas derivadas de las operaciones comerciales propias que no se pudieron realizar como consecuencia de la paralización del sistema).

Por otra parte, tampoco se podrá apreciar este delito si el perjuicio ocasionado no pudiese considerarse como grave, algo que, tal como también sucedía en el delito del artículo 264 CP, atendiendo a lo que exige la DAI, no supone ni puede suponer que el perjuicio producido tenga que superar los 400 €, sino tan solo que el mismo no pueda considerarse insignificante o irrelevante a efectos penales, determinando, por tanto, su absoluta atipicidad penal.

3.1.2. Tipo subjetivo

El artículo 264 bis CP contempla un delito doloso, con lo que, al encontrarnos de nuevo, como ya vimos, ante una figura de resultado-lesión, cabe la apreciación de su tentativa. Por otra parte, como sucedía en el delito anterior, también aquí parece que resulta aplicable la prescripción contenida en el artículo 267 CP, lo que abrirá las puertas a que se pueda castigar la comisión de este delito si se efectúa por imprudencia grave y concurren el resto de requisitos establecidos en dicho artículo.

3.2. Tipos cualificados

El artículo 264 bis CP contempla varios tipos cualificados que incrementarán la pena aplicable a aquel que realice la interferencia dolosa en sistemas informáticos que dicho precepto castiga.

En primer lugar, el propio artículo 264 bis.1 CP *in fine* obliga a aplicar la pena prevista para este delito en su mitad superior a aquellos sujetos que lo hubiesen cometido «perjudicando de forma relevante la actividad normal de una empresa, negocio o de una Administración pública». Esta prescripción protege especialmente las actividades de algunos de los posibles sujetos pasivos de este delito (empresas, negocios o administraciones públicas) atendiendo, a nuestro modo de ver, no solo al hecho de que estos suelen ser las víctimas más habituales de tales conductas, sino también y, sobre todo, a que su actividad tiene una trascendencia social que dota de mayor desvalor a su alteración (piénsese, por ejemplo, en los daños no patrimoniales derivados de la paralización de una administración o en la pérdida reputacional sufrida por la empresa víctima de este tipo de ataques).

Por otra parte, el apartado 2 del artículo 264 bis CP prevé la cualificación del delito aquí analizado en caso de que concurra en su ejecución cualquiera de las circunstancias cualificadoras del delito de daños en datos informáticos contempladas en el artículo 264.2 CP al que directamente se remite. Resultan, por tanto, plenamente trasladables aquí todas las consideraciones que se hicieron anteriormente al hilo del análisis de dichos tipos cualificados. Sin embargo, hay que reseñar que el artículo 264 bis.2 CP establece una pena significativamente mayor para la concurrencia de cualquiera de esas circunstancias con respecto al delito de daños por interferencia en sistemas informáticos de los que venimos hablando que el paralelo artículo 264.2 CP para el de daños por interferencia sobre datos o programas, diferencia sancionadora que ha sido tildada por algunos, no sin razón, de cuando menos sorprendente (Benítez Ortúzar, 2015), pero que determinará que en caso de que ambos tipos cualificados concurran con respecto a un mismo supuesto de hecho, se deba aplicar la aquí analizada atendiendo a su mayor pena.

Ved también

Para profundizar en las circunstancias cualificadoras véase el apartado «Tipos cualificados» del presente módulo.

De modo semejante, el artículo 264 bis.3 CP también permite incrementar la pena, tanto del tipo básico de este delito como de cualquiera de sus cualificados, si el daño en el sistema en cuestión se hubiese cometido utilizando datos personales ajenos para acceder al sistema informático o para ganarse la confianza de terceros, prescripción también completamente concordante con la establecida en el artículo 264.3 CP, por lo que nos remitimos a lo que allí dijimos con respecto a la misma.

Ved también

Véase el punto 7 del apartado «Tipos cualificados» del presente módulo.

4. Los daños informáticos terroristas

No queremos terminar esta breve exposición referida a los tipos cualificados aplicables a los delitos de daños informáticos sin comentar el hecho de que el artículo 573.2 CP establece que tendrán la consideración de delitos terroristas, con todo lo que ello implica, los contemplados en los artículos 264 y 264 bis CP cuando concurran en su realización alguna de las finalidades de las que habla el primer apartado de dicho artículo. Esto es, cuando se cometan con alguna finalidad terrorista. Cuando esto suceda, atendiendo a lo que establece el 573 bis.3 CP, se tendrá que aplicar a los responsables de tales delitos la pena superior en grado a la que esté generalmente prevista para el concreto delito de daños informáticos que hubiese cometido.

Pese a lo claro de esta prescripción, ha de reseñarse que si lo que determinase la consideración como terrorista de los delitos aquí analizados fuese el hecho de que se hubiesen realizado para desestabilizar gravemente el funcionamiento de las estructuras económicas o sociales de un país, como establece el artículo 573.1.1ª CP, mediante el daño de uno de los sistemas propios de las infraestructuras críticas, que precisamente sanciona el tipo cualificado del artículo 264.2.4ª CP, no se podría castigar, a nuestro juicio, a sus responsables aplicando simultáneamente la cualificación terrorista del artículo 573 bis.3 CP y la del referido tipo cualificado del delito de daños, dado que, al tener ambas cualificaciones un mismo fundamento, se encontrarían en una realización de concurso de leyes que nuevamente se habría de resolver por alternatividad.

5. La producción, adquisición o facilitación de instrumentos dirigidos a cometer daños informáticos

La última figura delictiva referida a los daños informáticos es aquella contemplada en el nuevo artículo 264 ter CP, precepto que, atendiendo a lo exigido por el artículo 7 de la DAI, viene a castigar a quien «sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

1) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o

2) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información».

Este delito resulta muy similar a otros contemplados en nuestro Código, como el contenido en el artículo 197 ter CP.

En concreto, castiga tanto producir (**crear**), adquirir para su uso (**comprar**), importar (**traer desde otro país**) o de cualquier otro modo facilitar a terceros (**entregárselos o transmitírselos**) de forma no autorizada programas informáticos concebidos o adaptados principalmente para cometer alguno de los delitos de los artículos 264 o 264 bis CP o bien hacer lo propio con las claves o códigos que permitan acceder a sistemas de información.

Estamos, sin duda, ante un nuevo tipo mixto alternativo que se podrá considerar realizado con la mera ejecución de una de sus conductas típicas sobre cualquiera de los objetos de los que su tipo habla, sin que la ejecución sucesiva y acumulada de varias sobre un mismo objeto y en una misma línea de ataque (por ejemplo, se crea el programa para cometer un delito y después se facilita a un tercero para que lo lleve a cabo) permita apreciar más de un delito.

Sin embargo, también estamos ante un tipo que solo podrá apreciarse si la realización de las conductas de las que habla recaen sobre unos elementos o instrumentos que se consideran especialmente peligrosos, se efectúan de forma no permitida y se hacen, además, con la finalidad de facilitar la comisión de alguno de los delitos de daños informáticos que hemos visto anteriormente.

Estos elementos típicos resultan fundamentales a la hora de apreciar este delito.

El primero de ellos lleva a que solo se pueda apreciar este delito si las actuaciones de las que habla se habían efectuado con respecto a un programa que haya sido creado o adaptado para que principalmente sirva para cometer alguno de los delitos de lo que venimos hablando o a las contraseñas, claves o datos similares que permiten acceder a sistemas de información (incluidos, por tanto, los datos biométricos cada vez mas utilizados por tales sistemas).

Creación de un programa

Por ejemplo, un virus, aunque también permite incluir entre ellos programas que puedan tener utilidades diversas a la delictiva, siendo dichas utilidades puramente marginales o secundarias.

Por su parte, la exigencia de que la actuación deba realizarse de forma **no autorizada** lleva a que no resulten típicas las actuaciones que se lleven a cabo de forma permitida por el ordenamiento jurídico (por ejemplo, la creación o adquisición lícita de programas por parte de la Policía destinados a bloquear webs por orden judicial).

Una vez que tenemos uno de estos instrumentos comisivos y se efectúa alguna de las conductas anteriormente señaladas de forma no permitida con respecto a los mismos, tendremos completo el tipo objetivo de este delito, que evidentemente se nos presenta como de mero peligro con respecto al bien jurídico que vendría a proteger, que sigue siendo, no lo olvidemos, el patrimonio.

Sin embargo, no basta con ello para poder apreciar este delito. Además, dicha actuación habrá de realizarse de forma **dolosa**, lo que, evidentemente, supone que su autor haya de conocer la naturaleza del instrumento en cuestión y el carácter no autorizado de la conducta efectuada con el mismo, y además, como ya hemos señalado, con «la intención de facilitar la comisión de alguno de los delitos de los artículos anteriores», es decir, con la finalidad de cometer o ayudar a cometer alguno de los delitos de daños de los artículos 264 y 264 bis CP.

Este especial elemento subjetivo del injusto, además de impedir que sea factible apreciar la comisión imprudente de este delito, lo convierte en una figura que viene a castigar, de forma autónoma y como delito consumado, lo que no serían sino actos preparatorios de la autoría o incluso de la participación de los comentados delitos. Convierte, en concreto, en delito autónomo algunas concretas conductas preparatorias de los delitos de los tipos cualificados de los artículos 264.2 y 264 bis.2 CP, lo que obliga a entender que si finalmente los instrumentos de los que habla el precepto aquí analizado fuesen utilizados de forma efectiva para cometer alguno de tales delitos, ya sea en su forma consumada o en mera tentativa, se tendría que apreciar el correspondiente concurso de leyes entre dicho delito y el aquí analizado. Un concurso que, aunque aparentemente debería solventarse atendiendo al **principio de consunción** en favor de la primera de las referidas figuras, tendrá que ser resuelto en cambio atendiendo al **principio de alternatividad** para evitar los problemas de proporcionalidad que se podrían generar si, atendiendo al de consunción, se castigase, por ejemplo, con menos pena al sujeto que crea un programa da-

ñino y lo utiliza sin llegar a producir la lesión que completan los injustos de los delitos de daños informáticos que al que simplemente lo hubiese creado sin haberlo siquiera empezado a emplear.

Un caso interesante en relación con esta materia es aquel que se refiere a la creación o suministro a terceros de aquellos programas que están primordial y casi exclusivamente diseñados para infectar ordenadores con el fin de que pasen a ser controlados remotamente por un tercero, integrándose así en una verdadera **red de sistemas *zombis* (*botnet*)**, que posteriormente será utilizada por dicho tercero para lanzar tal cantidad de peticiones de acceso o servicio al objetivo por él elegido que lo bloqueará, interrumpiendo así su funcionamiento.

Evidentemente si, en este tipo de casos, la actividad realizada es descubierta e interceptada antes de que se llegue efectivamente a utilizar la *botnet* para realizar el ataque que se pretendía efectuar, se tendrá que apreciar la completa comisión del delito aquí analizado. Esto es, del delito del artículo 264 ter CP.

Sin embargo, si el ataque se llega efectivamente a ejecutar, tendrá que apreciarse el correspondiente concurso de leyes entre la figura delictiva aquí analizada y el tipo cualificado de daños en sistemas informáticos del artículo 264 bis.2 CP que castigue la concreta participación que hubiese tenido en su realización quien creó o facilitó el programa utilizado para realizarlo, concurso que, evidentemente, también habrá de resolverse por alternatividad.

6. Cuestiones comunes

Señalar finalmente que el artículo 264 quater CP prevé la posibilidad de responsabilizar penalmente a las personas jurídicas por estos delitos, como exige el artículo 10 DAI, y que a estos delitos les son aplicables las prescripciones contenidas en los artículos 268 y 269 CP.

Esto último determina, en primer lugar, que queden exentos de penas los familiares, de los que habla el primero de los citados artículos, por los delitos de daños informáticos que cometan sin violencia, intimidación, ni abuso de superioridad y, en segundo lugar, que se puedan sancionar los actos de conspiración, proposición y provocación de la realización de dichas figuras delictivas.

Pese a ello, a nuestro modo de ver, deberá negarse la posible aplicación de lo establecido en el artículo 269 CP con respecto a la figura contemplada en el artículo 264 ter CP, ya que al castigar este precepto, como hemos visto, un mero acto preparatorio de otros delitos, si se aplicase lo establecido en el artículo 269 CP con respecto al mismo, se estarían castigando actos preparatorios de otros actos preparatorios, conductas cuyo castigo penal, al estar tan sumamente alejadas de la efectiva lesión de un bien jurídico de tan limitado valor como patrimonio, infringiría de forma manifiesta el principio de proporcionalidad.

Ejercicios de autoevaluación

1. La encriptación de un documento informático ajeno realizada sin autorización y de forma que impida acceder al mismo a su titular...

a) siempre será una conducta atípica.
b) solo será típica del delito de daños si determina que el documento en cuestión ya no resulte nunca más accesible.
c) solo será típica del delito de daños si recae sobre un documento que tenga un valor patrimonial superior a los 400 €.
d) no constituirá delito de daños si el documento en cuestión carece de valor patrimonial.

2. El delito de daños por interferencia en datos o programas informáticos...

a) solo puede cometerse de forma dolosa.
b) no admite la tentativa.
c) no puede ser apreciado cuando la conducta realizada recae sobre datos propios del sujeto que la realiza.
d) permite castigar los daños imprudentes que recaigan sobre programas informáticos que superen los 40.000 €.

3. La creación y efectiva distribución de un virus que haya llegado a borrar datos valorados en más de 20 millones de euros almacenados en más de dos mil ordenadores...

a) constituirá un delito del tipo básico de daños sobre datos informáticos del artículo 264.1 CP.
b) constituirá un delito de daños sobre datos informáticos del tipo cualificado del artículo 264.2.2º CP atendiendo a la gravedad de los daños ocasionados.
c) constituirá un delito de daños sobre datos informáticos del tipo cualificado del artículo 264.2.2º CP atendiendo al elevado número de ordenadores afectados.
d) constituirá un delito de daños sobre datos informáticos del tipo supracualificado del artículo 264.2 *in fine* CP atendiendo a la extrema gravedad de los daños ocasionados.

4. Si se borran algunos de los datos contenidos en un sistema informático de tal forma que el mismo ralentiza su funcionamiento y esto causa al titular del sistema una pérdida patrimonial grave...

a) nos encontraremos ante el delito de daños por interferencia en un sistema informático del artículo 264 bis.1 CP.
b) estaremos ante el delito de daños por interferencia en datos informáticos del tipo cualificado del artículo 264.2 CP.
c) habrá que apreciar un concurso de delitos entre a) y b).
d) solo constituirá delito en la medida en que la alteración del sistema realizada ocasione un perjuicio grave a un servicio esencial.

5. Si un sujeto crea un virus destinado a borrar determinados programas de un sistema informático y lo introduce en dicho sistema, ocasionando que tales programas se borren y que el sistema deje de operar, y esto produce un perjuicio patrimonial grave a su titular...

a) cometerá el delito de producción de instrumentos dirigidos a cometer daños informáticos del artículo 264 ter CP.
b) responderá del delito de daños sobre sistemas informáticos del tipo cualificado del artículo 264 bis.2 CP.
c) responderá de un concurso de delitos entre a) y b).
d) responderá de un concurso de leyes entre a) y b).

6. Si un grupo de sujetos se ponen de acuerdo para enviar desde sus ordenadores peticiones de acceso continuas a través de Internet al servidor de una empresa de ventas en línea y consiguen de esa forma que el acceso al servidor de tal empresa se sature y, por tanto, la entidad deje de poder vender sus productos en la red, paralizando de esta forma su actividad mientras dura el ataque, produciendo así un grave perjuicio económico...

a) responderán por el delito de daños sobre datos informáticos del tipo básico del artículo 264.1 CP.

b) serán responsables de la comisión del delito de daños sobre sistemas informáticos del tipo básico del artículo 264 bis.1 CP.
c) responderán del delito de daños sobre datos informáticos del tipo cualificado del artículo 264.2 CP, por la peligrosidad del medio utilizado en el ataque.
d) serán castigados por haber cometido el delito de daños sobre sistemas informáticos del artículo 264 bis.1 CP, pero en su modalidad cualificada por haber afectado a la actividad de una empresa.

Solucionario

Ejercicios de autoevaluación

1. d

2. c

3. d

4. a

5. d

6. d

Bibliografía

Andrés Domínguez, A. C. (2016). «Reforma de los daños». En: N. Rodríguez García; A. Carrizo González Castell; F. J. Leturia Infante (dirs.). *Comentarios a la reforma penal de 2015*. Valencia: Tirant lo Blanch.

Benítez Ortúzar, I. (2015). «De los daños». En: L. Morillas Cueva (dir.). *Estudios sobre el Código penal reformado. Leyes orgánicas 1/2015 y 2/2015* (cap. 19, págs. 599-612). Madrid: Dykinson.

Castro Corredoira, M.; Vázquez-Portomeñe Seijas, F. (2015). «La reforma de los delitos de daños: arts. 263, 264, 264 bis, 264 ter, 264 quáter, 265, 266.1 y 266.2 CP». En: N. Rodríguez García; A. Carrizo González Castell; F. J. Leturia Infante (dirs.). *Comentarios a la reforma del Código penal de 2015*. Valencia: Tirant lo Blanch.

Galán Muñoz, A. (2010). «El robo de identidad: aproximación a una nueva y difusa conducta delictiva». En: A. Rallo Lombarte; L. Arroyo Zapatero; I. Alamillo Domingo, y otros. *Robo de identidad y protección de datos* (págs. 169-198). Cizur Menor: Aranzadi.

Muñoz Conde, F. (2017). *Derecho penal. Parte especial*. Valencia: Tirant lo Blanch.

Quintero Olivares, G. (2016). «De los daños». En: G. Quintero Olivares (dir.); F. Morales Prats (coord.). *Comentarios al Código penal español* (tomo II, 7.ª ed.). Cizur Menor: Aranzadi.