DERECHO PENAL

El delito de daños informáticos. Análisis jurisprudencial

Jose Manuel SIERRA MANZANARES
Oficial de la Policía Municipal de Madrid de la Comisaría Principal de Policía Judicial de Tráfico

La primera regulación penal sobre los daños a programas o documentos electrónicos ajenos aparece con la LO 10/1995, de 23 de noviembre, del Código Penal, que viene a tipificarlos en el artículo 264.2, dentro de los daños cualificados, con el texto siguiente:

"*La misma que se impondrá (prisión de uno a tres años y multa de doce a veinticuatro meses) al que 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*".

El Código Penal ya contaba con una expresa mención a estos programas o documentos frente a sustracciones y apoderamientos (art. 278.1, delitos relativos al mercado y los consumidores) y en cuanto a la propiedad intelectual (art. 270), por lo que se hacía necesaria la regulación de su destrucción o inutilización. El delito de daños, propiamente dicho, constaba del tipo básico del artículo 263 y los tipos agravados de los artículos 264, 265 y 266.

Publicado el Convenio de Budapest sobre Ciberdelincuencia en noviembre de 2001 la regulación en España acerca de los daños informáticos se quedaba claramente insuficiente. Hacía falta una regulación específica de daños informáticos, puesto que, hasta ese momento, este tipo penal de daños se subsumía en el tradicional tipo de daños en la propiedad ajena. Era necesario un tipo penal específico, que incluyera sin género de dudas, los daños a los programas informáticos (softwares), los daños temporales de los sistemas lógicos, existencia del delito sin el "daño físico", atendiendo más que a la incolumidad de la sustancia de una cosa a la de su valor de uso real.

Más tarde, la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, del 12 de agosto de 2013, "*relativa a los ataques contra los sistemas de información*" (sustituyendo a la Decisión marco 2005/222/JAI del Consejo) daba el plazo para transponer en las legislaciones nacionales, lo indicado en ella, hasta el 4 de septiembre de 2015. La Directiva trataba de dar solución, a la amenaza creciente, en el entorno UE y resto de los países, a la posibilidad de ataques terroristas o de naturaleza política contra los sistemas de información. También, una de sus preocupaciones era el incremento exponencial de las agresiones a los sistemas informáticos con métodos cada vez más sofisticados.

El objetivo principal de la Directiva era "***aproximar las normas de Derecho penal de los Estados miembros*** *en materia de ataques contra los sistemas de información, mediante el establecimiento de normas mínimas relativas a la definición de las infracciones penales y las sanciones aplicables, y mejorar la* ***cooperación entre las autoridades*** *competentes, incluida la* ***policía***[1] *[...]*".

Así las cosas, España tuvo que modificar el código penal para adecuarlo a la Directiva. Algunos autores piensan que la transposición fue realizada de una forma precipitada y defectuosa, con escasa discusión y debate parlamentario[2], lo que produjo, prácticamente, una recepción o transposición literal y acrítica del Derecho Comunitario a nuestro Derecho interno.

1 Considerando Nº1 de Directiva 2013/40/UE del Parlamento Europeo y del Consejo, del 12 de agosto de 2013.

[2] Avelino Fierro Gómez (Fiscal Delegado, Fiscalía Provincial de León). *La Evolución de delitos informáticos en el Código Penal. págs. 21-25*. Centro de Estudios Jurídicos, 2015.

Finalmente, como consecuencia de la Directiva, en España se aprobó la Ley Orgánica 1/2015, de 30 de marzo, por la que se modificó el Código Penal. La redacción de aquel momento, que sigue estando vigente actualmente, es la siguiente:

"***Artículo 264.***

1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles ***datos informáticos***[3]*,* ***programas informáticos o documentos electrónicos***[4] *ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.*

2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.ª Se hubiese cometido en el marco de una organización criminal.

2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero".

Conforme a la Circular de la Fiscalía 3/2017, de 21 de septiembre[5], el legislador pretendió abarcar todas las posibles conductas susceptibles de afectar a los elementos informáticos, tanto aquellas que impliquen su destrucción, bien sea total o parcial, como aquellas otras que comporten una modificación -alteración- de los mismos que igual podría producirse por eliminación, supresión o borrado parcial del elemento afectado como por la incorporación de nuevos datos que impliquen la variación del alcance o contenido inicial de aquellos descubrimiento y revelación de secretos y los delitos de daños informáticos.

Respecto a la conducta de "*hacer inaccesible*", dice la fiscalía que abarca aquellos supuestos en los que la acción ilícita, ejercida sobre los datos y/o programas informáticos o documentos electrónicos, produce como consecuencia, sin afectar a la existencia o esencia de los mismos, la imposibilidad de acceder a ellos ya sea para conocer su contenido, para operar con ellos o, en general, para utilizarlos en cualquier modo. Un buen ejemplo de este efecto es el que produce el programa malicioso conocido como ***ransomware***, que restringe el acceso a determinadas partes o archivos del sistema infectado, generalmente a través de su cifrado, situación que, en principio, solo podría

[3] La Directiva 2013/40/UE define datos informáticos como "toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función".

[4] La Ley 59/2003, de 19 de diciembre, de firma electrónica, que ha sido derogada por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, definía los documentos electrónicos en su artículo 3.5 como "la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado".

[5] Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos.

solventarse, y así lo suele plantear el atacante informático, abonando el rescate que con esa finalidad reclama a sus víctimas.

"***Artículo 264 bis***.

1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:

a) realizando alguna de las conductas a que se refiere el artículo anterior;

b) introduciendo o transmitiendo datos; o

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

Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.

2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero".

En este tipo penal la Fiscalía remarca que consiste básicamente en lograr un resultado concreto, cual es la obstaculización o interrupción de la normal actividad de un sistema informático ajeno, de manera grave y a través de alguna de las acciones indicadas en el precepto.

Se trata, por tanto, de un delito de resultado en el que el elemento esencial es que se produzca la efectiva y grave obstaculización o interrupción respecto de un sistema informático[6] concreto.

VELASCO NUÑEZ, E.[7] expone que el ejemplo más conocido de este tipo delictivo es el "***mail bombing***", o bombardeo simultáneo de un correo electrónico que acaba bloqueándose al saturar su capacidad de respuesta. La acción sancionada es la interrupción, la obstaculización (no dañar como en el 264 CP), y su objeto, más que el dato, documento o programa, **es el sistema**, de manera que el ataque aquí incide más en la operatividad informática que en la afrenta que suponga la información afectada.

"***Artículo 264 ter***.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

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

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

---

[6] Acorde a la citada Circular 3/2017, y a la Directiva 13/40/UE, por sistema informático debemos entender *"todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento".*

[7] VELASCO NUÑEZ, E. *Delitos tecnológicos. Cuestiones penales y procesales*. Madrid: *Wolters Kluwer*, 2021, pág 76-89

Indica la Fiscalía que la realización de las conductas típicas a efectos de obtener o facilitar a otros la disponibilidad de estos programas, así como también de contraseñas de ordenador, códigos de acceso o datos que permitan el acceso a la totalidad o a una parte de un sistema informático, integrará esta conducta cuando quien así actúe no se encuentre debidamente autorizado para ello y, además se acredite la **intención de destinarlos** a la comisión de cualquiera de las conductas de **daños informáticos** anteriormente examinadas.

Para VELASCO NUÑEZ este **delito es de sospecha** que castiga el producir, adquirir para usar (no meramente detentar), importar o de cualquier modo facilitar a terceros, sin estar debidamente autorizados, con la finalidad de facilitar la de los delitos anteriores, programas informáticos, contraseñas, códigos...

- ANÁLISIS JURISPRUDENCIAL -

A continuación, se analizan una serie sentencias judiciales de diferentes tribunales, haciendo hincapié en detalles interesantes desde el punto de vista del derecho penal sustantivo.

⇒ **STS Pleno 91/2022, de 7 de febrero**

En los hechos probados se pone de manifiesto el comportamiento de un trabajador que, siendo despedido, un día antes de abandonar la empresa borró todos los archivos relacionados con la actividad que había desempeñado en relación con la zona comercial de Portugal, de la que en dichos momentos era el único comercial encargado. Borró varios archivos de Excel y Outlook (unos 700mb de información) relacionados con compras, proveedores, volumen marcas... sufriendo la empresa perjuicios económicos en el ámbito organizativo, y de prestigio al verse imposibilitada y dificultada para gestionar las ventas pendientes, así como el seguimiento y comunicación con los clientes del área de Portugal. La información no pudo ser recuperada ni existía una copia de seguridad. El Juzgado de lo Penal nº18 de Valencia condena al trabajador a 1 año y 6 meses de prisión por el artículo 264.1ºCP. La Audiencia Provincial de Valencia, asienta su absolución en que las consecuencias económicas del borrado no han sido cuantificadas ni de forma aproximada, y le absuelve. La empresa recurre la resolución de la AP. Finalmente, el Alto Tribunal vuelve a condenar al empleado exponiendo que "*la **gravedad típica se alcanza cuando es imposible recuperar la operatividad del sistema o cuando su recomposición es difícilmente reversible sin notables esfuerzos de dedicación técnica y económica**. Debe observarse que las unidades o procesos informáticos que aquí se protegen, son elementos intangibles que no siempre presentan un valor económico intrínseco [...]*". Cita, además el TS la SAP Madrid, Secc. 23ª, Nº23/2017, de 10 de enero, en la que se indica que "*el resultado grave de los daños causados en los datos informáticos deberá ser estimado caso por caso atendiendo a criterios que permitan apreciar esa gravedad, **criterios** como puede ser la **posibilidad o no de recuperar** los datos informáticos, la **pérdida definitiva** de los mismos o la posibilidad de recuperación y, en este último caso, el **coste económico** de la **reparación del daño** causado, la **complejidad técnica** de los trabajos de recuperación, la **duración de las tareas** de recuperación, el **valor del perjuicio** causado al titular de los datos, bien como lucro cesante o como daño emergente*".

⇒ **STS 220/2020, de 22 de mayo**

En los hechos probados un empresario comienza a desconfiar de uno de sus trabajadores por diversos motivos. Cuando el empresario se entera que el trabajador ha dicho "*no sabe con quien se las está buscando*" decide restringirle el acceso al programa informático de uso empresarial. El empleado permaneció en su despacho y aprovechó para acceder a su ordenador y usuario y borrar de su ubicación en la carpeta "escritorio" 54 carpetas que contenían 1074 archivos informáticos, de los que no existía copia de seguridad y que contenían documentos relacionados con el funcionamiento de la oficina. De dichas carpetas el trabajador era el único que disponía de permisos de administrador para poder borrarlas. Lo interesante de este supuesto, que podría parecer muy parecido al anterior es que la Audiencia Provincial de Badajoz le condena por un delito de daños informáticos en grado de tentativa (artículo 16 CP). Posteriormente el TS le absuelve. Expone el Alto tribunal varios puntos a reseñar, "*la primera conclusión a la que conduce el análisis del tipo es que los daños informáticos son atípicos cuando el resultado -en su descripción más básica- no es grave. Es cierto que se trata de un concepto normativo que **habrá de ser fijado***

sin aferrarnos a un criterio puramente cuantitativo que lleve, por ejemplo, a entender que esa gravedad, cuando no alcanza la frontera de los 400 euros, carece de relevancia típica". Es decir, la frontera de los 400€, a los que los policías estamos acostumbrados a tener en cuenta, en este delito deja de ser un requisito.

Otro tema tratado en la sentencia, interesante, es el de la tentativa. La Audiencia Provincial condena por tentativa indicando "*el delito lo ha sido en grado de tentativa pues aunque el acusado realizó todos los actos necesarios para la consumación del delito y sin embargo, el resultado no se produjo por causas ajenas a su voluntad ya que el sistema operativo guardó los archivos automáticamente en la papelera de reciclaje, de donde pudieron ser rescatados por el informático de la oficina lo que evitó in extremis la pérdida definitiva de dichos archivos*". **El TS admite la tentativa en este tipo de delitos**, pero indica que en los hechos acontecidos el trabajador hizo todo aquello que quería hacer *"[...] y esa acción produjo el resultado asociable a su verdadera entidad, que no es otro que el traslado a la papelera de reciclaje de los archivos borrados y su* ***eventual recuperación por todo usuario que así lo quisiera***", por lo que el delito en su caso se hubiese consumado. Finalmente, como se ha indicado el TS le absuelve porque los archivos eliminados que fueron a parar a la papelera de reciclaje eran de fácil recuperación, no siendo el resultado grave como exige el tipo penal, "*el borrado de 54 carpetas que incluyen 1074 archivos, que al ser eliminados se alojan en la* ***papelera de reciclaje*** *y sobre los que el acusado no vuelve a intentar ninguna acción destructiva,* ***no alcanza la relevancia típica exigida*** *por el art. 264.1 del CP*".

⇒ **SAP Barcelona, Secc. 7ª, Nº 766/2022, 16 de noviembre**

En esta sentencia se absuelve, nuevamente, a un trabajador. En este caso por la imposibilidad se acreditar que fuera él, no porque los hechos no fueran típicos.

Los Mossos d'Esquadra, elaboraron un informe que ratificaron en el acto del juicio en el que afirman que el usurario podía ser utilizado por cualquier persona que tuviera las claves de acceso, por lo que (a priori) no puede descartarse que el acceso lo realizara una tercera persona. Se genera una duda razonable acerca de la autoría, por lo que al Tribunal no le queda otra respuesta que la absolución.

Los hechos probados "*[...] utilizando una IP propiedad de JAZZTEL, persona que no ha podido ser identificada accedió al sistema informático de la empresa citada, mediante el uso del usuario DIRECCION00. Tal acceso tuvo las siguientes* ***consecuencias****: Los sistemas de virtualización fueron apagados, se trata de un sistema de máquinas virtuales, conjunto de equipos informáticos que ejercen de plataforma y soporte de todo el Software, que permite la correcta ejecución del proyecto, siendo afectado el correo corporativo que desapareció. Google España no facilitó los datos necesarios para poder determinar quién lo pudo manipular, por no contarse con orden judicial. Quedó afectado el sistema de edición de vídeos, creado por la empresa. Con la contraseña conocida no se podía entrar en la cuenta de los vídeos,* ***no pudiendo ser recuperados***".

⇒ **SAP Valencia, Secc. 2ª, Nº 497/2022, 7 de octubre**

En esta sentencia, un informático contratado por un empresario, una vez despedido, aprovechando el conocimiento adquirido en la realización de los programas en su etapa como trabajador, en menos de dos meses, accedió unas 50 veces a páginas de la administración de la aplicación gracias a los fallos de diseño y vulnerabilidades en la aplicación en cuanto al control de accesos y permisos, circunstancia que él conocía por haber desarrollado la programación. Efectuó numerosas acciones de borrado, modificó fórmulas que tuvieron que ser reconstruidas y se tardó por ello más tiempo en conseguir la plena operatividad del sistema, lo que motivó un costoso trabajo por parte del desarrollador de modelos y del informático de la empresa. Debido al ataque informático, la empresa no pudo ofrecer el producto en el un Congreso muy importante de su sector.

La sentencia indica que *"[...] no es fácil modular la gravedad de una acción sin la referencia que proporciona su resultado que, al exigirlo el legislador, ha de ser también grave. Se trata pues, de una* ***gravedad encadenada, acumulativa****, que no siempre podrá afirmarse sin dificultad.* ***Una manipulación limitada al simple pulsado de varias teclas y comandos puede propiciar daños informáticos de especial gravedad y que conduzcan a la inutilización del sistema. En tales casos, la levedad de la acción tendrá como punto de contraste la***

gravedad del resultado, suscitando fundadas dudas acerca de su tipicidad". Quizás lo interesante de esta resolución es que el Ministerio fiscal realizó su escrito de acusación por un delito continuado (artículo 74 CP) de daños informáticos. Sin embargo, la Audiencia elimina la continuación delictiva exponiendo que "*precisamente la gravedad, exigida en el tipo penal, determina que* ***estemos ante una unidad típica de acción, constitutiva de un solo delito y no de un delito continuado, aunque los accesos y ataques al programa informático se hayan producido en días sucesivos o muy próximos en el tiempo****. Además, tratándose de un mismo sujeto pasivo, de una misma* ***unidad de propósito y de daños*** *semejantes, ocasionados con cierta estrechez temporal, desde una dimensión socio- normativa, resulta lógico apreciar un único supuesto fáctico, subsumible en un único delito de daños*".

⇒ **SAP Málaga Secc. 3ª, Nº 209/2019, 24 de mayo**

Lo interesante es que la Audiencia incide en que este delito es autónomo y no puede catalogado nunca como delito leve por la cuantía de los daños. Expone "*no parece que el resultado grave deba ser identificado con una valoración del mismo superior a 400 euros que permita distinguir el delito menos grave del delito leve,* ***pues no existe una tipificación de esta figura penal como delito leve****. Como dice la SAP 345/2013 de 3 Junio de la Audiencia Provincial de Madrid, Sección 6ª, citada en la sentencia apelada, la frontera de los 400 euros establecida para diferenciar el delito de la falta de daños (art . 263 del Código Penal), no resulta de aplicación al delito de daños informáticos, recogido en el segundo número del art . 264 del Código Penal;* ***estamos ante un tipo penal autónomo****, diferenciado del delito de daños del art.263 CP con conductas típicas propias [...]*".

⇒ **SAP Palencia Secc. 1ª, Nº 42/2016, 14 de julio**

En los hechos probados dos personas a las que una fundación les adeuda dinero, con ánimo de menoscabar la propiedad ajena, entraron en una sala de control donde se encontraba la instalación informática que la mercantil de los acusados había montado junto con todo el sistema audiovisual necesario existente en las distintas salas, y sustituyó varias tarjetas de memoria que contenían archivos de audio e imagen, necesarios para proyectar la exposición, por otras tarjetas de memoria que no proyectaban correctamente la misma, de modo que resultaba imposible seguir la proyección. A consecuencia de ello la exposición se interrumpió durante cuatro meses, toda vez que, los acusados no entregaron las tarjetas necesarias para proyectar la exposición. Lo interesante de la sentencia es el requisito del "***animus nocendi***"[8] que requiere el tipo penal. La defensa de los dos acusados alega que no existe el ánimo de dañar, por lo que no existiría el tipo penal. Dice la Audiencia que "*poco recorrido jurídico tiene el argumento de que no se ha acreditado la existencia de daños ni ánimo de dañar, por cuanto los propios acusados tienen reconocido que cometieron los hechos sabiendo que,* ***como consecuencia*** *de ello, la exposición tendría que* ***interrumpirse****, con todas las* ***consecuencias económicas negativas*** *que iba a causar por que las personas interesadas ya no podrían visitar la exposición, previo pago de las entradas correspondientes, precisamente por ello sustituyeron las tarjetas para, de esta forma y conociendo los perjuicios económicos que se iban a producir, forzar a la Fundación a pagarles la cantidad adeuda. Además, a mayor abundamiento,* ***no olvidemos que el dolo, desde un punto de vista penal, no exige que sea específico pues basta con que sea de segundo grado e, incluso, eventual****, es decir,* ***aún*** *en el supuesto de que los acusados* ***no hubiesen buscado directamente la causación de daños****, lo que hay que poner en duda conforme antes hemos indicado,* ***basta con que los asumiesen*** *como resultado o consecuencia muy probable de su acción*". Leída la resolución de la Audiencia, queda clara una cosa, el tipo penal de daños informáticos es autónomo, requiere siempre (aún de forma eventual) el ánimo de dañar. No admite la modalidad imprudente, a diferencia de los daños básicos del artículo 263 CP, que admiten la modalidad por imprudencia grave (artículo 267 CP) cuando se cumplen unos requisitos de procedibilidad (requiere denuncia) y de cuantía (más de 80.000€), siendo en este caso un delito leve.

[8] Intención de causar daño

- CONCLUSIONES -

PRIMERA.- Los delitos de daños informáticos, son delitos perseguibles de oficio, no están sujetos a condiciones especiales de procedibilidad. No requieren denuncia del perjudicado para iniciar la acción policial y se deben realizar, acorde al artículo 282 LECrim., las diligencias necesarias para comprobarlos y descubrir a los autores.

SEGUNDA.- Para valorar el "resultado grave" de los daños del artículo 264 CP se debe atender a criterios de:

La probabilidad de recuperación de los datos informáticos.

La pérdida absoluta de los datos informáticos.

El coste económico de la reparación del daño.

La dificultad técnica que supone la recuperación.

TERCERA.- El resultado grave no responde a una valoración de la cuantía superior a 400€ para diferenciar entre el delito menos grave y leve. No cabe esa distinción. No existe el delito leve de daños informáticos, siempre será, al menos, delito menos grave. De aquí la importancia de diferenciar el delito de daños informáticos (configurado como un tipo penal autónomo) del de daños básicos (tipo básico del artículo 263 CP).

CUARTA.- El término "de manera grave" al que hace alusión el artículo 264 Bis CP ha de interpretarse en el sentido de que no toda obstaculización o interrupción del funcionamiento de un sistema se haría acreedora por si sola de una sanción penal, sino únicamente aquella que afecte realmente y de forma significativa a la funcionalidad del sistema atacado, circunstancia que será necesario analizar en cada supuesto en particular y que en un buen número de ocasiones precisará de los correspondientes informes técnicos.

QUINTA.- Los términos "sin estar autorizado" y sistema informático "ajeno" hacen que solo quede fuera de la competencia del CP cuando la actuación no necesite de autorización sobre el sistema informático, respecto del cual su titular tiene pleno control y disposición (conclusión 23ª Consulta Fiscalía 3/2017).

SEXTA.- Los programas informáticos producidos, adquiridos para su uso, importados o facilitados a terceros, mencionados en el artículo 264 Ter CP, han de estar concebidos o adaptados principalmente para la comisión de algunos de los delitos sancionados en los arts. 264 y 264 bis, al igual que las conductas típicas han de ejecutarse con esa misma finalidad.

SÉPTIMA.- El delito de daños informáticos admite el grado de tentativa cuando el autor dé principio a la ejecución del delito directamente por hechos exteriores, practicando todos o parte de los actos que objetivamente deberían producir el resultado, y sin embargo este no se produce por causas independientes de la voluntad del autor.

OCTAVA.- Los daños informáticos no admiten la modalidad imprudente, a diferencia del tipo básico del artículo 263 CP que pueden ser cometidos por imprudencia grave acorde al artículo 267 CP.

Bibliografía

FIERRO GÓMEZ, A., *La Evolución de delitos informáticos en el Código Penal*. Centro de Estudios Jurídicos. 2015.

GUTIERREZ MAYO, E. *Delitos informáticos paso a paso. Análisis de las conductas delictivas más comunes en el entorno informático*. A Coruña: Colex, 2021.

VELASCO NUÑEZ, E. *Delitos tecnológicos. Cuestiones penales y procesales*. Madrid: *Wolters Kluwer*, 2021.

Legislación

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

Ley 6/2020, de 11 de noviembre, *reguladora de determinados aspectos de los servicios electrónicos de confianza*.

Directiva 2013/40/UE del Parlamento Europeo y del Consejo, del 12 de agosto de 2013, *relativa a los ataques contra los sistemas de información*

Sentencias

STS Pleno 91/2022, de 7 de febrero.

STS 220/2020, de 22 de mayo.

SAP Barcelona, Secc. 7ª, Nº 766/2022, de 6 de noviembre.

SAP Valencia, Secc. 2ª, Nº 497/2022, de 7 de octubre.

SAP Málaga, Secc. 3ª, Nº 209/2019, de 24 de mayo.

SAP Palencia, Secc. 1ª, Nº 42/2016, de 14 de julio.

SAP Madrid, Secc. 23ª, Nº 23/2017, de 10 de enero.

Accede a nuestra tienda web y encuentra los manuales policiales operativos con el análisis operativo y la jurisprudencia más actualizada del mercado.