Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Facultad de Derecho

MÁSTER UNIVERSITARIO EN ABOGACÍA

TRABAJO FIN DE MÁSTER

ASPECTOS FUNDAMENTALES DEL DELITO DE DAÑOS INFORMÁTICOS Y RESPONSABILIDAD PENAL CORPORATIVA.

Alumna: Andreea Alexandra Florea

Convocatoria: Extraordinaria segundo semestre, junio 2022

RESUMEN

El objetivo de este trabajo de fin de máster es realizar un estudio de las diferentes facetas que presentan los delitos de daños informáticos con una breve referencia sobre el estado actual de la responsabilidad de la persona jurídica.

Recogerá los puntos comunes, como el bien jurídico protegido y la ajenidad de los bienes sobre los que recaen los ataques representativos de estos delitos, así como la caracterización específica de cada uno de los tipos penales que describen las diversas tipologías de los delitos de daños informáticos. Para ello se realizará un análisis de la normativa penal, tanto nacional como internacional, que dio origen a esta modalidad delictiva, así como de la actualmente vigente.

Asimismo, reflejará los inicios de la responsabilidad penal de las personas jurídicas y las líneas jurisprudenciales más relevantes, especialmente del Tribunal Supremo, que han ido aclarando esta nueva institución tras una regulación defectuosa. Finalmente, se hará un breve análisis del alcance de esta responsabilidad por la comisión de delitos informáticos, destacando la figura del *compliance officer*.

ABSTRACT

The aim of this master's thesis is to carry out a study of the different facets of computer crimes with a brief reference to the current state of the liability of the legal person.

It will include the common points, such as the protected legal right and the alien nature of the goods on which the attacks representative of these crimes fall, as well as the specific characterization of each of the criminal types that describe the various typologies of computer crimes. To this end, an analysis will be made of the criminal law, both national and international, which gave rise to this type of crime, as well as the current legislation in force.

It will also reflect the beginnings of the criminal liability of legal persons and the most relevant jurisprudential lines, especially of the Supreme Court, which have been clarifying this new institution after a defective regulation. Finally, there will be a brief analysis of the scope of this liability for the commission of computer crimes, highlighting the figure of the compliance officer.

ÍNDICE

ABREVIATURAS Y ACRÓNIMOS

Art ..... **Artículo**

Arts..... **Artículos**

CCN-CERT ..... **Centro Criptológico Nacional**

CD-ROM ..... **Disco Compacto**

CE..... **Constitución Española de 1978**

Coord ..... **Coordinador**

CP..... **Código Penal de 1995**

DDoS ..... **Denial of Service**

HOR..... **Human Operate Ramsonware**

ICAO..... **Ilustre Colegio de Abogados de Oviedo**

LECrim..... **Ley de enjuiciamiento Criminal**

LO ..... **Ley Orgánica**

Op.cit..... **Opere Citato**

Pág..... **Página**

RAM..... **Random Access Memory**

SS..... **Siguientes**

STS ..... **Sentencia del Tribunal Supremo**

TS ..... **Tribunal Supremo**

UE..... **Unión Europea**

VVAA..... **Varios Autores**

INTRODUCCIÓN.

Las nuevas tecnologías y la informática avanzan a pasos agigantados, mientras que la utilización de estas herramientas supone tanto ventajas como desventajas. Por un lado, conllevaría un trabajo minucioso exponer todas las ventajas que implican estos elementos intangibles, pero cabe mencionar la simplificación, la facilitación, la eficacia y la velocidad de la que disponemos a través de la automatización de todos los datos en la red. La aparición cada vez con más celeridad de nuevos componentes, dispositivos y herramientas informáticas representa un nuevo tipo de criminalidad, con un espectro delictivo amplio, difícil de seguir por la normativa y que de alguna manera se ha intentado regular en nuestro ordenamiento.

La tipificación de los delitos de daños informáticos, el objeto del presente trabajo, deriva de los compromisos internacionales adquiridos por España, sobre todo por la Directiva 2013/40/UE, de 12 de agosto de 2013, relativa a los ataques contra sistemas de información, de contemplar en su derecho nacional esta modalidad delictiva que presenta una característica pelicular: el desconocimiento y la dificultad que entraña localizar al autor de delito y su difícil detección por las víctimas del mismo.

El trabajo se estructura en cuatro capítulos en los que se presentará el análisis de los delitos de daños informáticos de forma sistemática, destacando los elementos comunes que presentan y las peculiaridades de cada uno de ellos, y una breve introducción a la responsabilidad penal de las personas jurídicas.

El primer capítulo se centrará en el estudio de los elementos objetivos y subjetivos del llamado delito de daños informáticos o sabotaje informático incorporado en nuestra normativa penal a través del art. 264 CP. Seguidamente, el segundo capítulo pondrá de relieven los mismos elementos en su vertiente de obstaculización o interrupción del funcionamiento de sistemas de información previsto en el art. 264 bis CP.

Teniendo en cuenta que para la comisión de los delitos de daños informáticos en ocasiones son necesarios diversos elementos o acciones que faciliten su perpetración, el tercer capítulo estará destinado al análisis del art. 264 ter CP que castiga las conductas destinadas a facilitar la comisión de aquéllos.

En el cuarto y último capítulo, analizaremos la incorporación de la responsabilidad penal de las personas jurídicas por delitos informáticos del art. 264 quáter CP junto con un breve

estudio de la incorporación y particularidades que representa la propia institución de la responsabilidad penal corporativa.

1.- EL DELITO DE DAÑOS O SABOTAJE INFORMÁTICO (ART. 264 CP).

1.1- INTRODUCCIÓN.

La primera referencia al delito de daños informáticos, más conocido como sabotaje informático, vino dada por el art. 264.2 CP aprobado por la Ley Orgánica 10/1995 que castigaba *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*. Aun incluyéndose en el precepto de subtipos agravados del delito de daños físicos y castigándose con penas similares, la naturaleza del sabotaje informático no era similar a la de los daños físicos, pues presentaba una característica particular: la afección a elementos inmateriales[1].

No fue hasta la reforma operada por la Ley Orgánica 5/2010, de 22 de junio cuando a esta modalidad delictiva se le otorgó independencia respecto de los daños físicos en el art. 264[2]. Posteriormente, la reforma introducida por Ley Orgánica 1/2015, de 30 de marzo supuso el germen de lo que hoy en día constituye esta figura delictiva[3], reorganizando sistemáticamente los preceptos dedicados, por un lado, en los comportamientos ilícitos destinados a dañar elementos informáticos concretos como son los datos, programas o documentos electrónicos ajenos y, por otro lado, en los destinados a obstaculizar o interrumpir el normal funcionamiento de sistemas informáticos.

De esta manera la normativa interna se adapta a la legislación europea que trata de forma diferenciada ambas modalidades delictivas. Mientras que la Directiva 2013/40/UE ofrece un tratamiento específico a la i*nterferencia ilegal en los sistemas de información* en el art. 4 respecto de la i*nterferencia ilegal en los datos* del art. 5, el Convenio de Budapest sobre la ciberdelincuencia, de 23 de noviembre de 2001 que trata por separado

[1] DE LA FUENTE TEJADA, E.: "La tipificación penal de los ataques a los sistemas informáticos" en Tratado de Derecho Penal Económico (dir. Antonio Camacho Vizcaíno), Madrid, 2019, Tirant lo Blanch, pág. 913.

[2] El origen de la modificación vino dado por la trasposición al ordenamiento jurídico español de la Decisión marco 2005/222/JAI del Consejo, de 24 de junio, sobre ataques a los sistemas de información. Con la reforma de 2010 se sancionaban los daños en datos, programas o documentos electrónicos ajenos e incluso la obstaculización o interrupción del normal funcionamiento de los sistemas informáticos ajenos.

[3] En este caso tuvo suma importancia la Directiva 2013/40/UE, de 12 de agosto, del Parlamento y del Consejo.

los *ataques a la integridad de los datos* en el art. 4[4] de los *ataques a la integridad de los sistemas* en el art. 5[5].

1.2- BIEN JURÍDICO PROTEGIDO.

Respecto al bien jurídico protegido de los delitos de daños informáticos, como ocurre en muchas ocasiones, la doctrina mantiene diversas posturas respecto al mismo.

En rasgos generales, los delitos informáticos abarcan todas las conductas delictivas que se llevan a cabo a través del uso de un elemento informático o vulneran los derechos de los propietarios de un elemento informático concreto. Como apunta RODRÍGUEZ MESA, el tema está en determinar si es necesario crear un nuevo bien jurídico protegido encaminado a brindar protección a la información almacenada, tratada y trasmitida a través de los sistemas informáticos, o si el bien jurídico protegido será determinado por la propia naturaleza de la infracción cometida[6].

Partiendo de esta base, autores como GONZÁLEZ RUS consideran que la aparición de nuevos objetos materiales del delito creados por la informática no son capaces de avalar la aparición de nuevos bienes jurídicos[7], mientras que CARRASCO ANDRINO considera que era necesaria la convocatoria de nuevos bienes jurídicos relacionados con la libertad y los intereses de seguridad, pues a raíz de la Decisión Marco 2005/222/JAI del Consejo, relativa a los ataques de los que son objeto los sistemas de información, de 24 de febrero de 2005, la sociedad de la información ha dado a luz a un nuevo bien jurídico: la seguridad de las redes y sistemas informático[8], que se define como *la capacidad de las redes o de los sistemas de información para resistir, como un determinado nivel de confianza, todos los accidentes o acciones malintencionado que*

[4] Art. 4 Convenio de Budapest, de 23 de noviembre de 2001: 1. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegitimo que dañe, borre, deteriore, altere o suprima datos informáticos.

[5] Art. 5 Convenio de Budapest, de 23 de noviembre de 2001: Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

[6] RODRÍGUEZ MESA, Mª. J.: "Los delitos de daños. Capítulo XI del Título XIII del CP tras la reforma de la LO 1/2015", Tirant lo Blanch, Valencia, 2017, pág. 60.

[7] GONZÁLEZ RUS, J. J.: "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet" en *Delito e informática: algunos aspectos. Cuadernos penales José María Lidón* (VVAA), *núm 4*, Universidad de Deusto, Bilbao, 2007, pág. 33.

[8] CARRASCO ANDRINO, M.: "El acceso ilícito a un sistema informático" en ÁLVAREZ GARCÍA F.J (dir., VVAA), *La adecuación del derecho penal español al ordenamiento de la Unión Europea. La política criminal europea*, Tirant lo Blanch, Valencia, 2009, pág. 344.

pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes o sistemas ofrecen o hacen accesibles[9].

Mayoritariamente la doctrina ha sostenido que el bien jurídico protegido es el propio de los daños que se causan sobre objetos corpóreos, es decir, la propiedad ajena. Sin embargo, señala DE LA MATA BARRANCO que son varias las voces que discrepan de esta teoría, alegando que podría tenerse un derecho de propiedad sobre el *hardware* que contiene los datos objeto de ataque o derechos de propiedad intelectual sobre determinados programas o bases de datos, pero no sobre los propios datos almacenados en el sistema, separando así su posible condición de sujeto pasivo del delito de daños sufridos por éstos, imposibilitando hablar de daños en propiedad ajena[10]. Resulta necesario en este último caso indicar que lo que realmente se protegen son intereses de tipo económico ya que esta conducta no solo afecta a la pérdida del valor económico de los datos que han sufrido el daño, sino que conllevan el inevitable perjuicio para la actividad empresarial que se desarrolla.

Apunta DE LA MATA BARRANCO, la cuestión reside en determinar si existe algo más allá de la protección de la propiedad al cometer un delito de sabotaje informático. Aun partiendo de la base, por un lado, de que el daño incide sobre los datos, documentos o programas almacenados en los sistemas informáticos y, por otro lado, que el concepto tradicional de daños supone la destrucción, desaparición o perdida de inutilidad o valor de una cosa, requieren de revisión *porque lo que importa es que se pueda acceder a tales datos, que se pueda disponer de ellos, en todo momento y, además, de modo íntegro, no que su valor teórico (su sustancia) quede incólume*, ya que como apunta el autor *no se trata de entender que se protege la información contenida en soportes informáticos porque tenga más valor en sí misma que otra información contenida en otros soportes, pero sí que ello se hace por la importancia que tiene individual y socialmente su integridad y accesibilidad al estar situada en redes o sistemas*

[9] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Seguridad de las Redes y de la Información: propuesta para un enfoque práctico, de 6 de junio de 2001, Bruselas, pág. 10. Disponible en: https://eur-lex.europa.eu/. Última conexión: 28.3.2022.

[10] DE LA MATA BARRANCO, N. J. y HERNÁNDEZ DÍAZ, L.: "El delito de daños informático, una tipificación defectuosa". *Estudios penales y criminológicos*, nº 29, 2009, pág. 326.

informáticos de los que hoy en día dependen todos los ámbitos públicos y privados, más allá del daño al dato o sistema concretos[11].

En definitiva, la doctrina se encuentra dividida respecto al bien jurídico a proteger, ya que mientras para algunos lo que se protege es la propiedad, otros son partidarios de la protección jurídica de la utilidad de la información almacenada en los datos o documentos del sistema informático, mientras que otros entienden que la protección jurídica se configura en torno a situaciones análogas a la propiedad en tanto el sujeto alega un interés inmediato en su integridad[12].

1.3- TIPO BÁSICO DEL ART. 264.1 CP.

1.3.1- CONDUCTAS TÍPICAS.

Art. 264.1: El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesible 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.

La actual redacción de este precepto detalla comportamientos como los de *borrar, dañar, deteriorar, alterar, suprimir y hacer inaccesible* que recaen sobre los *datos informáticos, programas informáticos o documentos electrónicos ajenos.* Estos términos pretenden incluir un gran abanico de conductas susceptibles de causar daños en los elementos informáticos que, aun siendo aparentemente sinónimos, hacen referencia a escenarios disímiles. En palabras de TEJADA DE LA FUENTE , siguiendo a GONZÁLEZ HURTADO, *los términos borrar y suprimir, aunque aparentemente sinónimos, hacen referencia a situaciones claramente diferentes, aplicándose el primero de ellos a los supuestos en los que el dato o datos informáticos afectados se hacen desaparecer visualmente pero continúan existiendo en el sistema, de forma tal que podrían ser recuperados en tanto que no sean eliminados mediante sobreescritura y, el segundo, a los casos de completa eliminación y desaparición de la información del*

[11] DE LA MATA BARRANCO, N. J. y HERNÁNDEZ DÍAZ, L, *op. cit.*, pág. 329.
[12] CORCOY BIDASOL, M.: "Protección penal del sabotaje informático. Especial consideración de los delitos de daños." *Diario La Ley*, 1990, nº. 1, 1000-1016. Disponible en: https://diariolaley.laleynext.es, última conexión 21.04.2022.

sistema atacado, mientras que *el término alterar, (…) es el cambiar la esencia o forma de algo o también el de estropear, dañar o descomponer, contempla una acción que puede producirse tanto por eliminación, supresión o borrado parcial del elemento afectado como por la incorporación de nuevos datos o informaciones que varíen su alcance o contenido inicial, circunstancia que habrá que interpretar en cada caso y a efectos de tipicidad a la luz de la exigencia de que la conducta genere un resultado grave*[13].

Respecto de la acción de *hacer inaccesible* dichos datos, programas o documentos informáticos, añade que *integra aquellos supuestos en los que la acción ilícita (…) sin destruirlos o dañarlos, produce como consecuencia la imposibilidad de acceder a los mismos bien sea para conocer su contenido, para operar con ellos o, en general para utilizarlos en cualquier modo*[14].

Como ya se adelantó anteriormente, estas acciones típicas recaen sobre los datos informáticos, programas informáticos y documentos electrónicos ajenos (*software*), no siendo necesario afectar de manera directa los dispositivos físicos (*hardware*) que permiten la transmisión o utilización de aquellos[15]; el problema que subyace en el resultado de la perpetración del delito de daños informáticos no repercute directamente sobre los objetos materiales en los que se almacena la información, sino que dicho resultado tendrá carácter exclusivamente inmaterial ya que afecta a la disponibilidad de la información, dañándola, alterándola, suprimiéndola o volviéndola inaccesible, afectando incluso la funcionalidad u operatividad del programa objeto del delito.

En definitiva, este delito abarca diversas conductas ilícitas cuyo punto en común es que utilizando una serie de procedimientos imposibilitan el uso de los datos, programas informáticos o documentos electrónicos, incluyéndose así en el concepto de daños *la afectación de la posibilidad de uso del objeto material sobre el que recae la acción* debido a que el *imposibilitar el uso del objeto material equivale al daño del mismo,* pudiendo hablar de esta manera de sabotaje, concepto amplio, que abarca no solo el daño, sino

[13] TEJADA DE LA FUENTE, E.: "La tipificación penal de los ataques a los sistemas de información" en CAMACHO VIZCAÍNO, A. (dir, VVAA), *Tratado de Derecho Penal Económico*, Tirant Lo Blanch, Valencia, 2019, pág. 917.
[14] TEJADA DE LA FUENTE, E., op.cit. pág. 918.
[15] De modo más específico, el *hardware* hace referencia a todos los componentes físicos del sistema informático (ordenadores, portátiles, CPU), mientras que el *software* engloba todas las aplicaciones, datos y programas que hacen funcionar o se ejecutan en el sistema informático. Los ataques informáticos pueden afectar a los dos indistintamente, pero la respuesta del Derecho Penal será diferente según se trate de uno u otro. DE LA MATA BARRANCO, N.J y HERNÁNDEZ DÍAZ, L., op. cit. págs. 312 y 313.

también otro tipo de actos cuyo efecto es el mismo, imposibilitar el uso del objeto material[16].

En este punto es necesario concretar algunas de las conductas que conllevan un resultado dañoso específico de este tipo de delitos. Estas conductas o ataques se llevan a cabo a través de los llamados *virus*, definidos por SERRANO FERRER como *aquel programa cuya finalidad es alterar el funcionamiento de un equipo informático sin el consentimiento del usuario (…) diseñados para dañar el equipo, borrando información esencial, inutilizando o eliminando programas, formateando el disco duro…etc*[17]. Siguiendo a esta autora, los virus comportan varias modalidades, como los gusanos, residentes virus de macro, troyanos, ejecutables o los *ramsonware*[18].

Ahora bien, para que este tipo de delitos sea susceptible de reproche penal, ya desde la LO 5/2010, de 22 de junio, es necesario que la conducta delictiva tenga consideración de grave y, en la misma línea, el resultado producido también sea grave. Dicho de otra manera, es necesario que tanto la conducta delictiva como el resultado del acto ilícito tengan la consideración de graves.

Partiendo de esta premisa, la conducta delictiva tendrá consideración de grave cuando sea apta para producir el efecto pretendido, mientras que el resultado se considerará grave una vez que se hayan utilizado una serie de parámetros como los que revelen, por ejemplo, que la trascendencia de aquél implica alteración, inutilización o destrucción, ya sea temporal o definitiva, de los elementos o documentos objetos del ilícito, los costes económicos necesarios para el restablecimiento de la operatividad de los objetos del delito, el perjuicio causado tanto a la víctima como al interés general, así

[16] MUÑOZ CONDE, F.: "Derecho Penal. Parte especial". Tirant lo Blanch, 23ª ed., Valencia, 202. Pág 462.
[17] SERRANO FERRER, Mª P.: "El reflejo de las nuevas tecnologías en el derecho penal y otros destellos". *Thomson Reuters Aranzadi*, 1ª Edición., 2016. Pág. 89.
[18] Se entienden por *gusanos* aquellos programas que residen en la memoria y se copian a sí mismos, de modo que colapsan en tráfico por la red (los más habituales son aquellos que se copian utilizando la libreta de direcciones de Microsoft Outlook y se envían a sí mismos como ficheros adjuntos o los que se propagan a través de los canales de IRC de modo que para activarse modifican el registro de Windows y cada vez que se ejecute un archivos con extensión .EXE., el virus se activa; a modo de ejemplo está el llamado gusano del arco iris de Twitter). Los *residentes* son aquellos que permanecen en la memoria RAM esperando que se den algunas condiciones para su activación y su posterior propagación para causar daños; desaparecen al apagar el ordenador, pero una vez encendido se vuelven a colocar en la memoria al modificar el registro de Windows; se propagan a través de CD-ROM, disquetes o adjuntos en e-mails (el ejemplo más común es el *virus 13* o *virus Jerusalén*). Los *virus macro* los encontramos en programas como Word o Excel. Los *troyanos* actúan a través de un programa aparentemente inofensivo, introduciendo el virus en el dispositivo ajeno permitiendo a otro sujeto tener control sobre el ordenador afectado. En cuanto a los *ramsomware*, son aquellos programas malintencionados que se caracterizan por el secuestro de ficheros. SERRANO FERRER, Mª P.: Op. cit. Págs.89-91.

como importancia o trascendencia de los bienes jurídicos objeto de lesión por la acción ilícita y, como apunta TEJADA DE LA FUENTE, criterios que revelen *el riesgo generado para los intereses públicos o privados por efecto de la pérdida o alteración de los datos, programas o documentos afectados*[19].

1.3.2-OBJETOS MATERIALES DE LA CONDUCTA: DATOS, PROGRAMAS INFORMÁTICOS Y DOCUMENTOS ELECTRÓNICOS AJENOS.

Analizada la conducta ilícita, es necesario el estudio de los objetos sobre los que aquélla recae: datos y programas informáticos y documentos electrónicos.

Atendiendo al tenor literal del art. 2 b) de la Directiva 2013/40/UE, se entiende por "datos informáticos" *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.*

Respecto del "programa informático" o *software*, se entiendo como un *conjunto de instrucciones que, una vez ejecutadas, realizan una o varias tareas en un ordenador o sistema, sirviendo para que el sistema de información realice su función*[20]. Resalta la Sección 2ª Audiencia Provincial de Valladolid en su sentencia 82/2020, de 8 de junio que para su punición es necesario que dicho programa informático sea *malicioso, diseñado especialmente para infiltrarse, obtener información y/o dañar un dispositivo o sistema de información sin el consentimiento de su propietario*.

Por su parte, el concepto de "documento electrónico" se recoge en la Decisión Marco 2005/222/JAI como *toda representación de hechos, informaciones o conceptos, expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función* y en el

[19] TEJADA DE LA FUENTE, E., op.cit. pág. 921. La propia autora plantea el problema que se suscita en torno al límite a partir del cual estos criterios son útiles para determinar qué hechos son merecedores de la consideración de graves. Resalta el considerando decimoprimero de la Directiva que expone que *un caso puede considerarse de menor gravedad, por ejemplo, cuando el daño causado por la infracción o el riesgo que acaree para intereses públicos o privados, como la integridad de un sistema o datos informáticos o los 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.*

[20] En esta misma línea, los arts. 95 y ss del Texto Refundido de la Ley de Propiedad Intelectual que regula los derechos de autor sobre determinados programas, los define *como toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.*

mismo sentido, en el art. 3.5 de la Ley 59/2003, de 19 de diciembre, sobre la Firma Electrónica, como *la información de cualquier naturaleza en forma electrónica, archivada en soporte electrónico, según un formato determinado y susceptible de identificación y tratamiento diferenciado*[21].

Para que la conducta que recae sobre estos elementos sea considerada ilícita se requiere, así como lo expresa el Audiencia Provincial de Valladolid en la sentencia anteriormente mencionada, que la acción del autor sea realizada sin autorización y que sea ajeno al objeto material, es decir, que el *autor carezca de disponibilidad respecto a los contenidos o sistema sobre el que actúa, de modo y manera que, como así afirma la Circular 2/2017, de 21 de septiembre de la Fiscalía General del Estado (…) sólo la actuación no necesitada de autorización sobre sistemas informáticos propios, respecto de los cuales su titular tiene pleno control de disposición, quedarían al margen de la aplicación de este precepto (…).*

No obstante, parte de los estudiosos de esta materia consideran que la introducción de este elemento de ajenidad suscita problemas de interpretación sobre todo cuando los elementos informáticos, que aun perteneciendo o hayan sido creados por personas concretas, se destinan a posteriori al uso compartido con una multitud de personas que trabajan en el mismo ámbito y utilizan como propio un sistema informático de modo diferenciado de unos respecto a otros, es decir, con diferente alcance y derechos sobre el mismo[22].

[21] Al respecto resulta ilustrativa la Resolución de 19 de julio de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.

[22] Tejada de la Fuente considera en este punto que no quedan muy claras las razones por las que el legislador introdujo este requisito ya que resulta evidente que un hecho tendrá relevancia penal cuando los derechos o intereses de terceros o colectivos resulten afectados, de modo que tales conductas de borrado o destrucción de elementos informáticos propios del sujeto quedarían excluidas del ámbito punitivo, salvo que se trate de una conducta lesiva de la obligación legal de conservación. Asimismo, la propia redacción del tipo penal puede considerarse redundante al exigir esta ajenidad por parte de quien actúa no estando autorizado para ello. Expone la autora que este requisito de ajenidad ha de interpretarse conjuntamente con el requisito de la falta de autorización, concretamente con *la falta de disponibilidad plena sobre los contenidos o sobre el sistema informático en el que se actúa de tal forma que resultarían típicas y por tanto susceptibles de sanción penal, siempre que concurran los restantes requisitos legales, aquellas acciones que se realizan con los objetivos indicados sin estar habilitado para ello, sobre elementos informáticos de los que no se tiene disponibilidad plena*. TEJADA DE LA FUETE, E., op.cit. Págs. 923 y 924.

1.3.4- ELEMENTO SUBJETIVO DEL DELITO.

De la propia redacción del art. 264.1 CP podemos constatar que la conducta delictiva se lleva a cabo de manera intencionada, independientemente de si se trata de dolo directo o de dolo eventual.

Respecto al dolo eventual, recuerda la Sala de lo Penal del Tribunal Supremo respecto del delito genérico de daños en su sentencia 97/2004, de 27 de enero que éste *no exige un dolo especifico; basta con un dolo de segundo grado e incluso un dolo eventual (STS NÚM. 722/95 de 3 de junio [RJ 1995, 4535] y núm. 30/01 de 17 de enero [RJ 2001, 397]). Existe el delito de daños aunque el culpable no buscase directamente la causación de los daños, bastando que los asumiese como resultado o consecuencia muy probable de su acción*.

Así, tanto de las normas europeas como del propio CP, podemos extraer que la ilicitud de las conductas realizadas sin autorización y de manera grave ha de ser entendida en el sentido de que el autor del hecho actúa con conocimiento de que no está autorizado para ello y además que aquel hecho es capaz de dañar significativamente los datos, programas informáticos y documentos electrónicos.

Por último, el art. 267 CP plantea la posibilidad de comisión del delito de daños informáticos por imprudencia, castigando indistintamente los daños causados por imprudencia grave cuando su cuantía supere los 80.000 euros. En un primer momento podría plantearse la comisión del delito de daños por imprudencia solamente respecto de los daños producidos a objetos materiales, pero teniendo en cuenta su ubicación y la falta de especificidad del legislador en las últimas reformas, lleva a mantener que la aplicación del art. 267 CP opera sin distinción alcanzando esta figura de tipo inmaterial aun cuando suscite dificultades para cuantificar los daños causados a partir de una cuantía determinada.

1.4- SUBTIPOS AGRAVADOS DEL ART. 264.2 CP.

1.4.1- AGRAVANTE ESPECÍFICA DEL APARTADO 2 DEL ART. 264 CP.

El segundo apartado del art. 264 CP reza así:

Art. 264.2 - 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.

El primer problema que se suscita se da en torno a la primera circunstancia agravante, cuando el delito se haya cometido en el marco de una organización criminal debido a que puede concurrir con el art. 570 bis del mismo cuerpo legal cuando el autor del delito de daños informático sea, asimismo, integrante o dirigente de la organización en cuyo seno se lleva a cabo la acción ilícita[23]. La Circular 2/2011 de la Fiscalía General del Estado, sobre la reforma del Código Penal por Ley Orgánica 5/2010 en relación con las organizaciones y grupos criminales da respuesta a este problema y se inclina por un concurso de normas cuya resolución viene dada por el art. 570 quáter in fine al determinar que *cuando las conductas previstas en dichos artículos estuvieren comprendidas en otro precepto de este Código, será de aplicación lo dispuesto en la regla 4ª del art. 8, debiendo,* recuerda la citada Circular, que de acuerdo con el criterio de alternatividad, *aplicar el tipo con pena más grave, esto es, el art. 570 bis*. Respecto de los grupos criminales han de aplicarse las reglas del concurso real de delito.

En cuanto a la segunda circunstancia agravante del delito cuando *haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos,* constatamos que se trata de dos escenarios distintos para cuya aplicación de la agravante no es necesaria la concurrencia de ambas. Para la aplicación de la primera situación es

[23] TEJADA DE LA FUENTE, E., op.cit. pág. 928.

necesario que concurran los requisitos del tipo básico, es decir, que los afectos del daño causado, por su gravedad, merezcan la consideración de especialmente graves, mientras que la segunda situación, se dará cuando los sistemas afectados por el delito sean un número elevado.

Por lo que respecta la tercera modalidad agravante, considera la doctrina, y en particular FERNÁNDEZ GARCÍA, que el *servicio esencial* es un concepto jurídico indeterminado[24] cuya valoración ha de ser contrastada atendiendo las circunstancias concretas en las que se mueve la sociedad, de modo que ha de velarse por aquellos servicios imprescindibles para el buen ejercicio de sus derechos y el funcionamiento básico de la sociedad conforme a los principio y valores del Estado[25]. Por su parte, la *provisión de bienes de primera necesidad* ha de ser entendida como bienes cuasi primarios que, conforme a la reiterada jurisprudencia del Tribunal Supremo, y en concreto en su sentencia 232/2012, de 5 de marzo, son aquellos productos básicos para la subsistencia, especificando que *la categoría de "cosas de primera necesidad" se encuentra referida a aquellas de las que no se puede prescindir, según el diccionario de la Real Academia, lo que esta sala viene vinculando a productos de consumo imprescindible para la subsistencia o la salud de las personas*. A grosso modo, estas agravantes operan cuando la comisión del delito perjudique gravemente, por un lado, el funcionamiento normal de los servicios esenciales para la sociedad y, por otro lado, el sistema previsto para abastecer a los ciudadanos de los bienes imprescindibles para su subsistencia[26].

La cuarta circunstancia agravante prevé asimismo dos situaciones distintas. Por un lado, cuando *los hechos hayan afectado al sistema informático de una infraestructura crítica*[27] y, por otro, cuando *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*, prevé asimismo dos situaciones diferentes.

[24] FERNÁNDEZ GARCÍA, Mª. Y. (2006) "Concepto jurídico indeterminado de servicio esencial en la Constitución española". *Revista de Administración Pública*, núm. 190, págs. 325-338.
[25] TEJADA DE LA FUENTE, E., op.cit. Pág. 934.
[26] TEJADA DE LA FUENTE, E., op. cit. Pág 936.
[27] Respecto de la circunstancia agravante que contempla las infraestructuras criticas resulta relevante la *Ley 8/2011, de 28 de abril, por las que se establecen las medidas para la protección de las infraestructuras críticas*, al contemplar en su Preámbulo que estas *infraestructuras suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden desencadenarse en cascada a través del propio sistema tienen la posibilidad de ocasionar fallos inesperados y cada vez más graves en los servicios básicos para la población.*

Es necesario indicar respecto de las *infraestructuras críticas* la existencia de un Catálogo Nacional de Infraestructuras Estratégicas, registro de carácter administrativo, que recoge la información detallada de todas las infraestructuras declaradas estratégicas en el territorio nacional, incluyendo también aquellas críticas europeas que afectan al Estado español[28], cuyo contenido es secreto. De ello derivan dificultades a la hora de analizar si el autor del delito conocía el carácter estratégico de dicha infraestructura.

El segundo inciso de la cuarta circunstancia agravante relativo a la creación de *una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea*, exige que para su observancia se haya producido una situación de peligro grave. Debido a la importancia de los organismos y de los bienes jurídicos afectados, expone la ya citada TEJADA DE LA FUENTE, que *habrá de considerarse la concurrencia de un delito de terrorismo, en atención a las finalidades pretendidas por los autores del hecho delictivo*, siendo de aplicación la consideración de ilícito terrorista *a todas las nuevas figuras típicas relacionadas con los ataques a los sistemas de información dado que a tenor de lo establecido en actual art. 573.2 CP cualquiera de los delitos sancionados por los arts. 197 bis y 197 ter y 264 y 264 quáter podrían adquirir esa consideración si se cometen con algunas de las finalidades recogidas en el art. 573.1 CP*, pudiendo producirse *un concurso de normas a resolver de conformidad con el art. 8.1 CP de acuerdo con criterios de especialidad dado que el propio art. 573.3 cualifica específicamente estos actos como terroristas en atención a dicha finalidad*[29].

Respecto de la última circunstancia agravatoria del delito, cuando *delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter*, hace referencia a los ataques informáticos en los que resultan dañados los datos, programas o documentos electrónicos ajenos una vez utilizadas herramientas específicas aptas para la comisión de dichos daños informáticos, herramientas tales como programas informáticos creados o adaptados para dicha finalidad en concreto o mediante contraseñas de ordenador, códigos de acceso o datos similares que permitan el acceso a la totalidad o a una parte de un sistema de información.

[28] El art. 4 de la Ley 8/2011, de 28 de abril establece que será el Ministerio del Interior, a través de la Secretaría de Estado de Seguridad y previa identificación por el Centro nacional de Protección de Infraestructuras y Ciberseguridad, el encargado del catálogo Nacional de Infraestructuras estratégicas

[29] TEJADA DE LA FUENTE, E., op. cit. Pág. 940.

1.4.2- AGRAVANTE ESPECÍFICA DEL APARTADO 3 DEL ART. 264 CP.

El último apartado del art. 264 CP dispone que:

Art. 264.3 - 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.

Tal y como se desprende del propio precepto, la circunstancia agravante se configura en torno a la utilización de datos personales de un sujeto, pudiendo tratarse de la propia víctima o de un tercero. Los datos personales han de entenderse en sentido amplio definiéndose en el apartado 1 del art. 4 del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE como toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.*

Esta agravante se puede apreciar incluso cuando los datos personales se utilices de forma ocasional o esporádica sin necesidad de ocasionar perjuicio alguno para el titular de tales datos personales[30], pero cuyo uso fraudulento facilita el acceso a un sistema.

[30] A diferencia de la regulación europea, el legislador ha omitido la exigencia de perjuicio al titular de la identidad usurpada. La Directiva 2013/40/UE contempla esta agravación cuando *se hubiesen utilizado ilícitamente datos de carácter personal de otra persona con la finalidad de ganar la confianza de un tercero, causando así daños al propietario legítimo de la identidad*.

2.- EL DELITO DE OBSTACULIZACIÓN O INTERRUPCIÓN DEL FUNCIONAMIENTO DE SISTEMAS INFORMACIÓN DEL ART. 264 BIS CP.

2.1- INTRODUCCIÓN.

Tanto el Convenio sobre la Ciberdelincuencia como la Directiva 2013/40/UE contemplan la obligación de los Estados miembros de implementar en sus ordenamientos medidas sancionadoras de las conductas que obstaculizan o irrumpen de manera importante el funcionamiento de un sistema de información. De esta manera la LO 1/2015 introdujo en el ordenamiento jurídico penal español el art. 264 bis, cuyo contenido reza así:

Art. 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, obstaculizará 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.

Para una correcta aplicación de este precepto resulta necesario que su interpretación se haga a la luz del art. 264 CP, por lo que constituirán delito del art. 264 bis CP las conductas de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos.

En consonancia con lo anteriormente mencionado, añade la Fiscalía General del Estado en su Circular 3/2017, de 21 de septiembre, que *muchas de las conductas que contempla el art. 264 bis son reconducibles a las acciones típicas sancionadas en el art. 264. 1 CP, por lo que en una pluralidad de ocasiones la aplicación de una u otra figura típica vendrá determinada por la capacidad de la acción ilícita para afectar a la operatividad del sistema informático en su conjunto*, de modo que tanto la introducción, como la transmisión de datos, destrucción, daño, así como la inutilización de un sistema informático a través de su sustitución conforma este tipo penal[31].

2.2- ELEMENTOS OBJETIVOS

2.2.1- TIPO BÁSICO DEL ART. 264 BIS 1º CP.

2.2.1.1- CONDUCTA TÍPICA.

De conformidad con la línea trazada en el apartado anterior, la conducta típica de este delito viene constituida por un resultado: la obstaculización o interrupción grave de un sistema informático[32].

Detalla RODRÍGUEZ MESA que se trata de un delito de resultado material alternativo que puede producirse a través de medios específicos, pero también alternativos, pudiendo consistir en la *realización de algunas de las conductas contemplada en el art. 264 CP; en la introducción o transmisión de datos informáticos; y destrucción, daños, inutilización, eliminación o sustitución de un sistema informático, telemático o de almacenamiento de información electrónica*[33].

Las conductas consistentes en obstaculizar e interrumpir un sistema informático coinciden con las premisas decretadas en el art. 4 de la Directiva 2013/40/UE:

Interferencia ilegal en los sistemas de información. Los Estados miembros adoptarán las medidas necesarias para que la obstaculización o la interrupción significativas del funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo

[31] GUTIÉRREZ MAYO, E.: "Delitos informáticos Paso a paso. Análisis detallado de las conductas delictivas más comunes en el entorno informático". Colex Reader, 1ª Edición, 2021. Pág. 61.
[32] Los tres textos legislativos, el CP de 1995 (art. 264, la Directiva (art. 4) así como la Convención de Budapest (art.5) lo detallaban con los mismos términos, con la salvedad del último precepto que utiliza el verbo obstaculizar y no interrumpir para determinar el efecto que ha de producir la consecución del delito sobre el sistema informático atacado.
[33] RODRÍGUEZ MESA, Mª. J. Op. cit., pág. 92.

inaccesibles datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

Por su parte, las conductas relativas a la interferencia de datos se amplían con las acciones de introducir o transmitir datos en el art. 264 CP y art. 5 de la Directiva:

Interferencia ilegal en los datos. Los Estados miembros adoptarán las medidas necesarias para que borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

De este modo, cualquiera de las conductas previstas en el art. 264 CP que se refieran a los datos informáticos pueden dar lugar al resultado típico previsto en el art. 264 bis CP. Como ejemplo, uno de los métodos de ataque más común es el *ransomware*[34], que ya no solo se manifiesta mediante el envío de un código dañino que encriptan los archivos del sistema hasta que se pague un rescate, sino que cada vez es más frecuente su versión sofisticada de *HOR* (*Human Operated Ransomware*) que amenazan a la víctima con hacer públicos los datos sustraídos en partes de la Dark Web[35].

Otro de los ataques que están en el alza según los organismos nacionales son aquellos cuyo principal objetivo son el funcionamiento de los sistemas, más conocidos como *DDoS* (*Denial of Service*, ataques distribuidos de denegación de servicios) a través de los cuales se introducen o se trasmiten datos informáticos[36].

La tercera modalidad de está dirigida contra el propio sistema informático, y aunque no esté prevista como tal en la Directiva, el legislador español optó por incorporarla con la finalidad de poder considerar típicos aquellos comportamientos en los que el resultado previsto en la norma se produce a consecuencia de un ataque propiamente dicho contra los sistemas informáticos, como podría ser el caso de un corte de suministro eléctrico que interrumpe el buen funcionamiento del sistema informático[37].

Un elemento muy relevante es la calificación de la conducta. El legislador exige para que la conducta adquiera carácter delictivo que la obstaculización o interferencia en

---

[34] Concreta el Centro Criptológico Nacional que los *ransomware* más activos son los *Maze, LockBit, Ragnar Loker, Ragnarok, NetWalker, Nemty, Tycoon, SNAKE, Avaddon, Thanos, Phobos, Black-Kingdom, DoppelPaymer, REvil, TinyCryptor, Ryuk, RansomExx, Conti, Egregor, Pay2Key o Zeppelin*. Ciberamenazas y tendencias. Análisis de las ciberamenazas nacionales e internacionales, de su evolución y tendencias. Edición 2021, CCN-CERT (Centro Criptológico Nacional). Pág. 42. Disponible en https://www.ccn-cert.cni.es/. Última conexión: 28.03.2022.

[35] Ciberamenazas y tendencias. Op. cit. Pág. 30 y 41.

[36] Ciberamenazas y tendencias. Op. cit. Pág. 51.

[37] RODRÍGUEZ MESA, Mª. J. Op. cit. Pág. 92 y 93.

los sistemas informáticos haya sido realizada de forma grave. Se prescinde de la gravedad del resultado, de modo que la obstaculización o interferencia se convierten en el elemento central de la conducta delictiva independientemente del resultado que derive de la misma. Por lo que respecta a las condiciones en las que la conducta merece la calificación de grave, nos remitimos a lo señalado en el apartado 1.3.1 de este trabajo, añadiendo al respecto la FGE en su Circular 3/2017 *que no toda obstaculización o interrupción del funcionamiento de un sistema informático se haría acreedora por si sola de una sanción penal, sino únicamente aquella que afectara realmente y de forma significativa 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*.

2.2.1.2- OBJETO MATERIAL DE LA CONDUCTA: SOFTWARE DE SISTEMA.

El art. 264 bis CP castiga las conductas que recaen sobre el buen funcionamiento de los sistemas informáticos atribuyendo su objeto material al *software* del sistema.

Para que la conducta sea delictiva, el *software* atacado ha de ser ajeno. La concurrencia de este requisito puede darse en dos circunstancias: ya sea cuando el *software* sea completamente ajeno al sujeto que lo manipula, ya sea cuando, aun siendo su creador o titular, éste carece de disponibilidad, total o parcial, por concurrir con él otros sujetos ligados al contenido o funcionamiento del *software*[38].

El concepto de sistema de información descrito en la Directiva 2013/40[39] se aplica a cualquier sistema informático, aunque no todo sistema de información es un sistema informático. Concreta la Directiva que se trata de *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 dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento.*

En este sentido, concreta RODRÍGUEZ MESA que la conducta delictiva recae sobre *cualquier sistema informático que se utilice para obtener, almacenar, manipular,*

[38] TEJADA DE LA FUENTE, E., op. cit. Pág. 953 y 954.

[39] Artículo 2 Directiva 2013/40. Definiciones A efectos de la presente Directiva, se aplicarán las definiciones siguientes: a) «sistema de información»: todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento auto mático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento;

administrar, controlar, procesar, transmitir o recibir datos, para satisfacer una necesidad de información[40].

Por último, los ataques recaídos sobre el sistema informático pueden darse sobre cualquier componente del *software* de sistema, como pueden ser los sistemas operativos (Windows, Linux)[41], controladores de dispositivos (Drivers)[42], herramientas de diagnóstico (Everest, Antivirus)[43], herramientas de corrección y optimización (Ccleaner), servidores (FileZilla, WampServer)[44] o los programas utilitarios (RedoBackup).

2.3- ELEMENTO SUBJETIVO DEL DELITO.

Al igual que ocurría en el delito anterior, la conducta no autorizada y grave, exigencia del precepto a examinar, supone que el sujeto que actúa de esta forma debe ser consciente de que la conducta que está realizando tiene la capacidad o el potencial de alterar significativamente el funcionamiento normal del sistema y que no está autorizada en tiempo y forma para actúar de esta manera.

Poniendo estos dos preceptos sistemáticamente, el art. 264 CP y art. 264 bis CP, en el ámbito del artículo 267 del mismo texto legal, los daños pueden ser perseguidos por culpa grave cuando la cuantía supere los 80.000 euros y concurran las condiciones de perseguibilidad previstas en el artículo 267: *sólo serán perseguibles previa denuncia de la persona agraviada o de su representante legal. El Ministerio Fiscal también podrá denunciar cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida*.

---

[40] RODRÍGUEZ MESA, Mª. J. Op. cit. Pág. 91.

[41] Un sistema operativo es un conjunto de programas que permite manejar la memoria, disco, medios de almacenamiento de información y los diferentes periféricos o recursos de nuestra computadora, como son el teclado, el *mouse*, la impresora, la placa de red, entre otros. Recuperado de: https://desarrollarinclusion.cilsa.org/.

[42] Un controlador de dispositivo es una pieza de *software* que permite al sistema operativo y programas interactuar adecuadamente con dispositivos de *hardware* anexados al ordenador. Recuperado de: https://www.alegsa.com.ar/.

[43] La herramienta de diagnóstico es un tipo de software de utilidad que permite evaluar el correcto funcionamiento de uno o más aspectos del *hardware* o *software* de un dispositivo informático o de servicios informáticos. Recuperado de: https://www.alegsa.com.ar/.

[44] En redes, un servidor es un ordenador central en un sistema de red que provee servicios a otros ordenadores. En internet, los servidores son proveedores de todos sus servicios, incluyendo WWW en las páginas web, el FPT, el correo electrónico, los grupos de noticias, aplicaciones web, etc. Todos estos servicios y otros son provistos por uno o más ordenadores conectados a internet, encargados de recibir el requerimiento. El servidor analizará el requerimiento, lo procesará y enviará un resultado. Recuperado de: https://www.alegsa.com.ar/.

Como suele ocurrir con estas figuras delictivas, la falta de autorización constituye un elemento esencial de la ilegalidad del hecho. Dicha autorización puede ser legal, reglamentaria o basada en una relación contractual o una concesión o consentimiento de una persona habilitada para ello[45].

2.4- SUBTIPOS AGRAVADOS DEL ART. 264 BISCP.

El art. 264 bis CP prevé en su segundo apartado que:

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.

Esto implica que los subtipos agravados del art. 264.2 CP son aplicables, ya no solamente a los ataques contra aspectos específicos de un sistema de información, sino que además inciden de manera grave en el normal funcionamiento del propio sistema.

Cabe destacar que a pesar de que los criterios aplicables, aun siendo similares a las conductas previstas en el art. 246.1 CP, y teniendo en cuenta que los efectos de la acción ilícita pueden recaer sobre elementos aislados del sistema informático o produzca la obstaculización o interrupción de su normal funcionamiento, las penas a imponer son más graves que la general prevista en el primer apartado del art. 264 bis CP.

Como consecuencia, el art. 264.2 bis CP impone una pena privativa de libertad de tres a ocho años y una multa del triplo al décuplo del perjuicio ocasionado, muy superior, por un lado, a la pena de prisión de dos a cinco años y multa de del tanto al décuplo del perjuicio ocasionados prevista en el art. 264.2 CP respecto de las conductas del art. 264.1 CP y, por otro lado, a la pena máxima de prisión de al menos cinco años prevista en la Directiva 2013/40 para este tipo de delitos cuando se hayan desarrollado en el seno de una organización criminal o hayan producido daños de tal magnitud que afecten a los sistemas informáticos de infraestructuras críticas o de la máxima pena de prisión de al menos tres años en el resto de los casos.

Por su parte, el apartado 3 del art. 264 bis CP, dispone que:

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

[45] TEJADA DE LA FUENTE, E., op. cit. Pág. 955.

utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

En relación con esta agravante específica resulta de aplicación el mismo análisis que se ha realizado respecto del subtipo agravado del art. 264.3 CP.

3.- EL DELITO DE ABUSO DE DISPOSITIVOS DEL ART. 264 TER CP.

El art. 264 ter CP contempla:

Art. 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.

El legislador español, teniendo en cuenta que la consecución de los delitos contemplados en los art. 264 y 264 bis CP depende en ocasiones de elementos de hacking, contempla este delito de forma autónoma y castiga la producción, adquisición, importación o facilitación programas informáticos destinados a la comisión de los delitos contemplados en los preceptos mencionados, o de una contraseña de ordenador, un código de acceso o datos que facilite el acceso, ya sea en parte o en su totalidad, a un sistema de información.

La mera tenencia de estos elementos sin la realización de la conducta típica no da lugar a reproche penal. Por el contrario, si la tenencia está destinada a la comisión de los delitos de sabotaje o interferencia ilegal en los sistemas informáticos será de aplicación lo dispuesto en el art. 264. 2 5ª CP. Asimismo, detalla RODRÍGUEZ MESA que en el caso de que la interferencia ilegal no se produzca por circunstancias ajenas a la voluntad del autor del delito, serán de aplicación los art. 264 y 264 bis CP en grado de tentativa en su vertiente agravada.

La facilitación de los elementos contemplados en los apartados a) y b) de este artículo, así como lo detalla, puede ser de cualquier modo, incluyendo la distribución,

entendida como la transmisión de datos o programas, y la puesta a disposición, referente a la colocación de dispositivos en línea para el uso de terceros[46].

En el presente caso, los programas informáticos son aquellos confeccionados para alterar o destruir datos o interferir en el funcionamiento de los sistemas, excluyéndose del ámbito de aplicación los llamados *dispositivos de doble uso* que se destinan a usos civiles y militares. Para que el hecho sea constitutivo de delito se exige que la conducta se haya cometido sin autorización y con la finalidad de perpetrar la comisión de los delitos previstos en los art. 264 y 264 bis CP. De este modo, el reproche penal se constituye en torno a la falta de autorización y en la intencionalidad de comisión del delito que presenta dos rasgos: *una intención general de diseñar o adaptar el dispositivo para que objetivamente sea idóneo para la comisión de los delitos a los que hace referencia y una intención especifica de llevar a cabo la acción típica para cometer algunos de esos delitos*[47].

Por lo que respecta a las contraseñas de ordenador, códigos de acceso o datos, no se exige el requisito general de intencionalidad, consumándose el delito con la simple realización de la conducta ilícita.

Teniendo presente la circunstancia agravante del art. 264.2. 5ª CP, ésta absorbe por aplicación del art. 8.3 CP la *adquisición para su uso* contemplada en el art. 264 ter CP cuando el delito se haya consumado. El delito de sabotaje informático en grado de tentativa en relación con el delito de abuso de dispositivos también en grado de tentativa da lugar a un concurso de normas, que de conformidad con el art. 8.4 CP se resuelve mediante la aplicación de la norma que contempla la pena más grave, siendo ésta la prevista en el art. 264.2 5ª CP atenuada en uno o dos grados.

Por último, el hecho de que el sujeto *facilite a terceros* los elementos previstos en el precepto sin que haya cometido directamente el delito no lo exime de responsabilidad, sino que podrá considerarse cooperador necesario o cómplice de estos delitos.

[46] RODRÍGUEZ MESA, Mª. J. Op. cit. Pág. 95 y 96.
[47] RODRÍGUEZ MESA, Mª. J. Op. cit. Pág. 95.

4. ESPECIAL CONSIDERACIÓN SOBRE LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS POR DELITO DE DAÑOS INFORMÁTICOS.

4.1- INTRODUCCIÓN.

Antes de analizar las particularidades que entraña la responsabilidad penal de las personas jurídicas por esta modalidad delictiva, resulta necesario el estudio básico de diversos componentes que engloba la responsabilidad penal de ésta como tal. Entre ellos se enumera el nacimiento de la responsabilidad penal de la persona jurídica, sus modelos o sistemas de atribución los supuestos en los que una persona jurídica puede ser imputada y la situación procesal de ésta.

La responsabilidad penal de las personas jurídicas es una institución jurídica relativamente reciente en España, de las que más se ha hablado en los últimos años, quizás porque ha roto una de las grandes tradiciones seculares de nuestro Derecho Penal, *societas delinquere non potestas.* Se trataba de un axioma a través del cual se consideraba que una sociedad no podía delinquir. Con la reforma operada en el año 2010 del CP se rompe este principio básico construido en toda la parte dogmática penal que pensaba que la única persona que podía delinquir era la persona física. Surge en nuestro derecho algo que no se sabe si llega a conmover los cimientos de la dogmática penal, pero sí a cambiar la consideración de lo que un jurista debe pensar a lo que se debe de aplicar el derecho punitivo en nuestro país y en otros.

Así, con la LO 5/2010, de 22 de junio, junto con la reforma operada por la LO 1/2015, de 30 de marzo, se cambia la postura primitiva por obligación internacional, por las obligaciones contraídas por España en un primer momento con la UE[48], así como por el propio ordenamiento jurídico español. Consideraban los estudiosos que existe una triple motivación para imponer castigos a las personas jurídicas que se respaldan, por un lado, en *la concepción de la empresa como foco de delincuencia* (la mera existencia de una organización puede incrementar la generación de comportamientos individuales desviados), por otro lado, en *la necesidad de involucrar a socios y altos directivos en la prevención de comportamientos delictivos en el seno de la empresa* (impulsar a la persona jurídica hacia la autorregulación a través de códigos de conducta o *compliance programs*

[48] Se impulsó a los EM de la UE a adoptar una serie de medidas sancionadoras proporcionadas, eficaces y disuasorias, pero ni las directivas ni las decisiones marco imponían que esta responsabilidad fuera penal, pudiendo ser meramente administrativas.

para prevenir la comisión de delitos) y, por último, en *la necesidad de incrementar la eficacia del proceso penal* (la posible sanción que pueda imponerse a la persona jurídica además de prevenir la comisión de delitos, puede facilitar la investigación de los delitos que se han cometido y no han podido ser evitados)[49]. Como apunta FERNÁNDEZ TERUELO, las intervenciones legislativas derivadas de las actuaciones delictivas en el ámbito de empresa evitaron recurrir a fórmulas que induzcan al concepto de responsabilidad penal de la persona jurídica [50] como tal.

En España la responsabilidad penal de la persona jurídica se configura como una responsabilidad absolutamente autónoma de la responsabilidad penal que se le pueda exigir a la persona física, aunque se exijan conjuntamente en un proceso. Por otro lado, se determinó un sistema de incriminación *numerus clausus*, en base a la cual solamente se le pueden atribuir una lista cerrada y tasada de delitos a la persona jurídica, declarando en este sentido el art. 31 bis CP que las personas jurídicas serán penalmente responsables solamente de los delitos que prevean expresamente dicha responsabilidad. Es necesario señalar que la naturaleza de los posibles delitos imputables a la persona jurídica es dolosa, pudiendo en algunos casos ser culposa, se eleva el nivel de exigencia a la persona jurídica aunque los delitos se cometan de forma negligente por la persona física, existiendo una mayor exigencia de control o de que impida la comisión de los delitos en casos de negligencia.

Los supuestos en los que una persona jurídica puede ser imputada, siguiendo el art. 31 bis CP, puede darse en dos casos. Antes de concretarlos, cabe señalar que el CP no ofrece definición específica de los que se entiende por persona jurídica, debiendo

[49] MOIG ALTOZANO M.: "La responsabilidad penal de las personas jurídicas: societas delinquere et puniri potest", *Noticias Jurídicas,* 2012, pág. 1.
[50] FERNÁNDEZ TERUELO J. G.: Parámetros interpretativos del modelo español de responsabilidad penal de las personas jurídicas y su prevención a través de un modelo de organización o gestión (compliance). Incluye un análisis de los modelos de responsabilidad penal de las personas jurídicas en México y Ecuador. 1ª Edición, Aranzadi Thomson Reuters 2020, pág. 25.

acudir a la legislación civil[51], y en su caso a la mercantil[52], para determinar su concepto, pues no toda persona jurídica es penalmente imputable.

Volviendo al tema que nos ocupa, una persona jurídica puede ser imputada, de acuerdo con el art. 31 bis CP, en un primer momento, cuando los delitos sean cometidos por una persona física y que esta actúe en nombre o por cuenta de la persona jurídica, en beneficio directo o indirecto y siempre que sea representante legal o miembro de un órgano colegiado o individual que tenga posibilidad de comprometer o estar autorizada para tomar decisiones en nombre de la persona jurídica y ostenten facultades de organización o control. Se tratan de los representantes que hacen que dicha sociedad se vivifique y se mueva en el mundo jurídico. En un segundo supuesto, la persona jurídica será responsable cuando la comisión de los delitos no haya sido obra de las personas anteriormente mencionadas, sino por las personas dependientes de las mismas, es decir, sus empleados. Se trata de las personas que están sometidas a estos órganos por la propia jerarquía empresarial, cuando cometan un delito y cuando la causa de la comisión del delito sea la falta de vigilancia o control de los órganos encargados de realizarla.

Todo ello conlleva dos aspectos. En primer lugar, a la exención a la que después nos referiremos y, en segundo lugar, a cuál es la naturaleza jurídica de este tipo de responsabilidad.

Con la reforma de 2010 cuando se introduce la responsabilidad penal de las personas jurídicas se hablaba de transferencia de responsabilidad, o de la llamada heterorresponsabilidad o responsabilidad vicarial. Así, conforme la redacción inicial de

[51] El Código Civil en su artículo (art.) 35 define qué es la persona jurídica precisando, en primer lugar, que son *las corporaciones, asociaciones y fundaciones de interés público reconocidas por la ley*, matizando que *la personalidad* de éstas comienza *desde el instante mismo en que, con arreglo a derecho, hubiesen quedado válidamente constituidas* y, en segundo lugar, *las asociaciones de interés particular, sean civiles, mercantiles o industriales, a las que la ley conceda personalidad propia, independiente de cada uno de los asociados.* En este sentido conviene destacar que el Tribunal Supremo en su sentencia de 30 de septiembre de 1975 señaló *respecto a la naturaleza de las personas jurídicas (…) que son aquellos entes colectivos a los que se les reconoce capacidad de derecho patrimonial, para la consecución de un fin social durable y permanente; y en armonía con esta orientación legislativa, nuestro Código Civil, les reconoce una capacidad análoga a la de las personas individuales (…).*

[52] La Ley de Sociedades de Capital en su art. 33 determina que *con la inscripción la sociedad adquirirá la personalidad jurídica que corresponda al tipo social elegido,* otorgando así confiere personalidad jurídica una vez inscrita la sociedad de capital y el Código de Comercio regula el contrato de compañía mercantil, matizando que, una vez constituida de acuerdo con las reglas determinadas por el propio Código, será entonces cuando ésta adquiera personalidad jurídica, desprendiéndose así del art. 116 del CCom que dispone que *el contrato de compañía, por el cual dos o más personas se obligan a poner en fondo común bienes, industria o alguna de estas cosas, para obtener lucro, será mercantil, cualquiera que fuese su clase, siempre que se haya constituido con arreglo a las disposiciones de este Código. Una vez constituida la compañía mercantil, tendrá personalidad jurídica en todos sus actos y contratos*.

la reforma de 2010, los sujetos que podían generar responsabilidad penal de las personas jurídicas eran, por un lado, sus representantes y administradores de hecho o de derecho que hubieran cometido algún tipo delictivo en nombre o por cuenta de la aquellas y en su provecho y, en segundo lugar, las personas que estuvieran bajo el mando de aquellos representantes o administradores, cuando hayan cometido un delito en el ejercicio de su actividad por no haberse ejercido el debido control sobre ellos. En este caso si una persona física cometía en las condiciones anteriores un delito en el marco de una persona jurídica se transfería automáticamente la responsabilidad a la persona jurídica.

Siguiendo esta misma línea, el sector doctrinal se dividió en dos posiciones. Por un lado, existía la posición doctrinal que consideraba que el art. 31 bis contenía el llamado *modelo de trasferencia o atribución derivada de la persona física* que ha cometido el delito, sirviendo de base para negar la responsabilidad directa de la persona jurídica, más conocido como *sistema vicarial* o de trasferencia y expresa de la tipicidad. Este criterio fue seguido por la Circular 1/2011 de la Fiscalía General del Estado que en definitiva suponía que la persona jurídica responde por los delitos cometidos por las personas físicas (representantes o administradores de hecho o de derecho) en nombre o por cuenta de aquella y en su provecho. Por otro lado, otro sector doctrinal consideró que el modelo vicarial supone un modelo de responsabilidad objetivo ya que el principio de culpabilidad es uno de los principios básicos del Derecho penal[53].

En 2015 este asunto evoluciona y se considera que se trata de una responsabilidad propia de la persona jurídica, es decir, que se trata de autorresponsabilidad. Entre los puntos más trascendentales de esta modificación cabe destacar la intención de dejar atrás el modelo instaurado en la reforma anterior e incidiendo más en el delito corporativo. No obstante, así como manifiesta CADENA SERRANO, no está claro que esta barrera se haya conseguido ya que el modelo sigue siendo de responsabilidad de atribución o transferencia, dependiendo aun de la comisión del delito por parte de una persona física que la represente o sirva[54], tesis contraria que sostiene MARCHENA GÓMEZ al

[53] GRANADOS PÉREZ C.: "Posición del Tribunal Supremo sobre la responsabilidad penal de las personas jurídicas" en Fiscalía General del Estado (coord..), *La responsabilidad penal de las personas jurídicas: Homenaje al Excmo. Sr. D. José Manuel Maza Martín*, 2018, pág. 202.
[54] CADENA SERRANO F. Á.: "El estatuto penal de la persona jurídica" en *La responsabilidad penal…* op. cit., pág. 41.

descartar la responsabilidad vicarial debido a que la pena que se le impone a la persona jurídicas depende del hecho propio[55].

La doctrina del TS que gradualmente se ha ido construyendo sobre la responsabilidad penal de las personas jurídicas destaca que es criterio necesario para condenar a una persona jurídica, además de acreditar que el hecho delictivo ha sido cometido por una persona física dependiente de ésta, que la persona jurídica haya realizado una conducta delictiva, es decir, que haya cometido un delito corporativo al no instaurar las medidas adecuadas para detectar y evitar la comisión de delitos en su seno[56]. Todo ello conforma el denominado *defecto de organización* al que se le añade el *defecto de cumplimiento,* señalando SERRANO ZARAGOZA que *la atribución de responsabilidad penal a una persona jurídica exige la concurrencia de dos tipos de hechos que deben quedar acreditados: a) El tipo objetivo […]; b) Imputación subjetiva. Se trata del denominado doctrinalmente hecho propio de la persona jurídica, que no es otra cosa que el denominado defecto de organización de la persona jurídica cuyo estudio conviene ahora abordar. En conclusión, con la exigencia legal de que concurra –como presupuesto para atribuir responsabilidad penal a una persona jurídica– el defecto de organización, el legislador español ha situado nuestro modelo patrio de atribución de responsabilidad penal a las personas jurídicas en el ámbito de los modelos de autorresponsabilidad o responsabilidad por hecho propio*[57].

La primera sentencia sobre la responsabilidad penal de las personas jurídicas es la STS 514/2015, de 2 se septiembre en la que se planteó la posible extensión de los efectos favorables a la persona jurídica de un recurso de casación planteado por una persona física. Fue el primer momento en que el TS determinó que *se opte por un modelo de responsabilidad por el hecho propio, ya que por una fórmula de heterorresponsabilidad, parece evidente que cualquier pronunciamiento condenatorio de las personas jurídicas habrá de estar basado en los principios irrenunciables que informan el derecho penal*[58].

---

[55] MARCHENA GÓMEZ M.: "La contribución del magistrado José Manuel Maza a la consolidación de un modelo de autorresponsabilidad penal de las personas jurídicas" en *La responsabilidad penal…*op. cit., pág. 245.

[56]BANACLOCHE PALAO J. "Dilemas de la defensa, principios de oportunidad y responsabilidad penal de las personas jurídicas", *en La responsabilidad penal de las personas jurídicas: Homenaje al Excmo. Sr. D. José Manuel Maza Martín*, (coord. Fiscalía General del Estado), 2018, pág. 15.

[57] SERRANO ZARAGOZA O.: "Compliance penal y responsabilidad civil y societaria de los administradores" (coord. RUIZ DE LARA M.), Ed. Wolters Kluwer, Madrid, 2018, pág. 35.

[58] Con la sentencia 154/2016, de 29 de febrero, el TS ha desvirtuado el sistema vicarial, exigiendo que se acredite el delito propio de la persona jurídica cuya responsabilidad se exige, debiendo la acusación probar, por un lado, la conducta delictiva de las personas físicas y, por otro lado, la ausencia de un control eficaz destinado a prevenir o detectar el delito, línea jurisprudencial que coincide con la Circular 1/2016, de 22 de

Respecto a la situación procesal de la persona jurídica, afirmaba NAVARRO MIRANDA que plantea varios problemas en los tribunales penales españoles. Como señala BANACLOCHE PALAO, la Ley de Enjuiciamiento Criminal (LECrim) regulaba todo el proceso penal bajo la premisa de que el sujeto que cometía el delito era una persona física, pudiendo a la entrada en vigor de la LO 5/2010 exigir responsabilidad penal a las personas jurídicas, pero sin ninguna norma que contenga las directrices bajo las cuales pueda ser juzgada; nada indicaba cómo debía ser tratada ni los derechos de los que gozaba[59]; , no se especificaba ni cómo, ni cuándo, ni porqué, ni que derechos tenía, ni que derechos dejaba de tener, ni ninguna norma procesal. Posteriormente, la Circular 1/2011, de 1 de junio de la FGE dio una serie de pautas procesales, pero el desacierto legislativo se intentó compensar con la Ley Orgánica 37/2011, de 10 de octubre, de medidas de agilización procesal, que procuró equiparar *mutatis mutandis* la situación procesal de las personas jurídicas a las personas físicas y, como muy bien dice GÓMEZ COLOMER, no sabemos muy bien cómo. La principal norma fue la establecida en el art. 14 bis LECrim. De conformidad con este precepto, la competencia que derive por la imputación que se realice por el Ministerio Fiscal por el tipo de delito que sea imputable a la persona física, esa arrastra a la persona jurídica.

Naturalmente, la persona jurídica debe nombrar un representante, sin tener que ser necesariamente un representante orgánico de la sociedad. Se trata de un representante ad hoc, pudiendo cambiarlo en cualquier momento del procedimiento, con la salvedad de un impedimento legal: no puede tratarse de una persona jurídica o, de conformidad con el

---

enero al exponer *que si el fundamento de la imputación es la defectuosa organización societaria y esta se configura como elemento del tipo o define su culpabilidad, la acusación deberá probar, además de la comisión del delito por las personas físicas de las letras a) y b) del apartado primero, que tal infracción se ha cometido a consecuencia del ineficiente control de la persona jurídica. Otro entendimiento -que la persona jurídica estuviera obligada a probar su adecuado sistema de organización- representaría una inversión de la carga de la prueba constitucionalmente inadmisible.* En este mismo sentido se pronuncia el TS en su sentencia 221/2016, de 16 de marzo al exigir que se acredite el incumplimiento grave de los deberes de supervisión, que indisputablemente desprende consecuencias para la parde acusada ya que no todo delito cometido por parte de sus directivos supone un delito propio, sino que la acusación queda obligada a acreditar dicho incumplimiento grave.

[59] Ante la falta de regulación procesal, la doctrina comenzó a proyectar en cierta forma un tratamiento procesal de la persona jurídica en el proceso penal y también respecto de los derechos fundamentales que necesariamente han de acompañar a los imputados y acusados; todo ello a la luz de la doctrina del Tribunal Constitucional y de la jurisprudencia del Tribunal Supremo sobre estas cuestiones, pero respecto de las personas físicas. El legislador trató de solventar esta problemática a través de la reforma operada por la LO 37/2011, de 10 de octubre, de medidas de agilización procesal, modificando la LECrim respecto de la competencia, comparecencia, ejercicio de defensa rebeldía, presencia en el acto del juicio y conformidad, pero sin dar una respuesta completa a todas las dudas que hoy en día se siguen planteando. BANACLOCHE PALAO J.: "Dilemas de la defensa, principios de oportunidad y responsabilidad penal de las personas jurídicas", *en La responsabilidad penal de las personas jurídicas: Homenaje al Excmo. Sr. D. José Manuel Maza Martín*, (coord. Fiscalía General del Estado), 2018, pág. 13 y 14.

art. 786 bis LECrim, aquella persona llamada en condición de testigo por el Ministerio Fiscal o por la acusación. Asimismo, el TS en su sentencia 154/2016, de 29 de febrero planteo la posibilidad de compatibilidad en el caso de que la persona física imputada sea a la vez el representante de la persona jurídica imputada. En este caso, concreta el tribunal que esta equivalencia no está prohibida por la ley, sin embargo, el juez instructor y el tribunal sentenciador deben de apreciar que no haya contradicción de intereses entre uno y otro[60]. Asimismo, tienen derecho a nombrar abogado y procurador y, a diferencia de lo que ocurre con la persona física, la persona jurídica puede ser condenada en rebeldía.

Por último, respecto a la naturaleza jurídica de la carga de la prueba puede ser de carácter sustantivo y otra de carácter más adjetivo en lo referente al momento procesal en que es necesario hacer efectiva la prueba de la eximente.

La Circular 1/2016 estableció estos criterios al concretar que el principio general depende de la acusación que es la que debe probar la existencia del delito, la antijuricidad, la culpabilidad, los elementos que se constituyen y las posibles agravantes, mientras que la defensa debe de probar los eximentes. Bajo esta tesis estamos ante un supuesto de heterorresponsabilidad, el TS en su sentencia de 26 de febrero de 2016 considera la tesis opuesta, argumentando que se trata de autorresponsabilidad, pues la consideración del *compliance* como eximente es, sin embargo, un elemento del tipo negativo y, por lo tanto, los elementos del tipo lo deben probar la acusación.

Para concluir esta parte, siguiendo a NAVARRO MIRANDA, resultan interesantes dos posturas que mantienen GÓMEZ-JARA DÍEZ y GONZÁLEZ-CUELLAR SERRANO. Mientras que GÓMEZ-JARA DÍEZ establece una especie de artificio para solucionar el problema, de cada una de las partes deben de probar "algo", la acusación debe de probar que las medidas de control y de vigilancia en el caso concreto no han sido las óptimas y, por tanto, se debería de proceder a la absolución de la persona jurídica, y en el caso contrario, si de las pruebas resulta que las medidas de vigilancia y control no han sido las idóneas, la parte de la defensa debe de probar que estos sistemas de prevención, vigilancia y control de compliance era lo que la ley establece, ser suficientemente eficaces para la reducción de comisión de delitos; GONZÁLEZ CUELLO, lo considera una discusión "absurda", pues considera que se trata de una

[60] Detalla la mencionada sentencia que en caso de contradicción de interese se debe evitar que la persona física pueda ser representante legal de la persona jurídica. En muchas ocasiones puede producirse la conformidad de la persona física, pudiendo ser perjudiciales los hechos respecto de los cuales se conforma para la persona jurídica.

cuestión de beneficio de la duda, lo que implica que la defensa debe suscitar la duda de la eximente y el tribunal tendría que absolver si la duda radica en la existencia de la suficiencia del compliance, debiendo ser la acusación la que tenga que desvirtuar la duda que puso de manifiesto la defensa.

4.2.- RESPONSABILIDAD CRIMINAL CORPORATIVA PREVISTA EN EL ART. 264 QUÁTER CP Y LA FIGURA DEL COMPLIANCE OFFICER.

El art. 264 quáter CP expone que:

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los tres artículos anteriores, se le impondrán las siguientes penas:

a) Multa de dos a cinco años o del quíntuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años.

b) Multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, en el resto de los casos.

Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

Con independencia de que se trate de grandes corporaciones o de PyMES dedicadas a las nuevas tecnologías, resulta evidente que el uso de éstas es propicio para la comisión de actividades delictivas o con la finalidad de causar daños a terceros competidores.

El art. 264 quáter CP se remite a las situaciones previstas en el art. 31 bis CP analizado en el apartado anterior para la determinación de la responsabilidad penal de la sociedad. Con la reforma de la LO 1/2015 se introdujeron dos características fundamentales, que el delito se haya perpetrado en su *beneficio directo o indirecto*, detallando la Circular 1/2016 que "la sustitución…del término "provecho" por el de "beneficio directo o indirecto" despeja las dudas en favor de la interpretación lata que permite extender la responsabilidad de la persona jurídica a aquellas entidades cuyo objeto social no persigue intereses estrictamente económicos, así como incluir los beneficios obtenidos a través de un tercero interpuesto (caso de las cadenas de

sociedades), los consistentes en un ahorro de costes y, en general, todo tipo de beneficios estratégicos, intangibles o reputacionales"; y la exclusión de la responsabilidad penal de aquella cuando con anterioridad a la comisión del hecho delictivo se hubiera adoptado y ejecutado un sistema de *compliance* con la finalidad de prevenir el delito cometido.

Tratándose de sociedades cuyo objeto social puede estar comprometido o en riesgo de comisión de los delitos descritos en los arts. 264 y ss CP, deberán contar con un programa de *compliance* que contenga una identificación de riesgos TIC destinados a la *integridad y disponibilidad de los datos y sistemas informáticos una estructura normativa basada en normas y procedimientos tales como, por ejemplo, las políticas de Seguridad de la Información y una estructura de control y supervisión idóneas para prevenir y detectar tales delitos*[61].

La correcta implantación de los modelos de organización y gestión pueden exonerar de responsabilidad penal a la persona jurídica, de modo que ésta responderá penalmente cuando las facultades de supervisión, control y vigilancia no se han llevado a cabo. Así como apunta RODRIGUEZ MESA, la reforma operada en el año 2015 no se refiere a la figura del *compliance officer* una vez establecida la obligación de supervisión y vigilancia, tácitamente coinciden con las funciones propias de este cargo, surgiendo así el planteamiento de la responsabilidad del *compliance officer* por comisión por omisión.

Teniendo en cuenta que figura del *compliance officer* se ha convertido en el núcleo del cumplimiento normativo en la dirección de las empresas, como su propio garante, cumple con el requisito objetivo de la autoría en el tipo de comisión por omisión previsto en el art. 11 a) CP. Debido a la obligación contractual de actuar, en caso de comprobar la omisión típica y la consecución de alguno de los resultados descritos en los delitos por los arts. 264 y ss CP, si el resultado fuera imputable debido a la omisión conforme a criterios de la imputación objetiva, el *compliance officer* será autor de los daños informáticos en condición de autor por comisión por omisión.

El apartado a) del art. 31.1 bis CP abre la vía de responsabilidad penal de la persona jurídica cuando los daños informáticos la beneficien directa o indirectamente, pues la figura de *compliance officer* ostenta facultades de control dentro de la misma. Por el contrario, si no se ha obtenido el beneficio directo o indirecto de la persona jurídica, se podrá exigir responsabilidad penal al *compliance officer* sin transferir su responsabilidad penal a la sociedad que, sin embargo, sí podría ser responsable civil solidaria.

[61] RODRÍGUEZ MESA, Mª. J. Op cit. Pág 99.

Lo más destacable de la redacción de este precepto es la imposición de un sistema mixto para la cuantificación de la multa a la persona jurídica autora del delito en cuestión, de modo que rige el mecanismo de fijación de la sanción pecuniaria de días multa (de dos años a cinco años en caso de daños más graves o de un año a tres años en los demás casos) o si la cuantía resultara de mayor importe una vez valorado económicamente el daño causado por la acción ilícita. Dado que la normativa de la UE exigía a los EM tomar medidas que garanticen que las sanciones impuestas a las personas jurídicas sean efectivas, proporcionadas y disuasorias, el art. 264 quáter CP otorga la posibilidad a los jueces y tribunales a imponer las penas recogidas en el art. 33.7 b) a g) CP conforme a las reglas establecidas en el art. 66 bis CP[62].

En los supuestos más graves la multa proporcional puede evolucionar desde el doble al triple o hasta el quíntuplo a doce veces más en los supuestos más graves o del triple a ocho veces más en los daños de menor cantidad[63].

[62] RODRÍGUEZ MESA, Mª. J. Op cit. Pág. 101.
[63] CASTRO CORREDOIRA. M. y VÁZQUEZ-PORTOMEÑE SEIJAS, F.: "La reforma de los delitos de daños: arts. 263, 264, 264 bus, 264 ter, 264 quáter, 265, 266.1 y 266.2 CP" en GONZÁLEZ CUSSAC J.L(dir., VVAA), *Comentarios a la Reforma del Código Penal de 2015*, 2ª ed., Tirant lo Blanch, Valencia, 2015, pág 799.

CONCLUSIONES

Tras el estudio del tema principal del presente trabajo, se pueden extraer el siguiente colofón y una breve opinión personal.

PRIMERO. – Los avances tecnológicos pueden ser caracterizados por los grandes beneficios de los que disfruta la sociedad, pero también representan la cuna de una nueva categoría delictiva como lo es la de los daños informáticos. Los delitos de carácter informático se han convertido en una de las bases de la criminalidad en nuestros tiempos. Poseen el poder de causar estragos económicos en una línea temporal muy limitada, al mismo tiempo que pueden implicar la afectación de otros derechos de carácter personal como puede ser la propia intimidad de las personas que lo sufren.

SEGUNDO. –Si bien la denominación penal de esta modalidad delictiva es de *daños informáticos*, quizás el término adecuado sería *sabotaje informático* debido a que al tratarse de nuevas formas de criminalidad realmente no presentan características que posibiliten su encaje en los tipos penales tradicionales. De este modo, el sabotaje informático se convierte en la versión informática de los delitos de daños previstos en los arts. 264 y ss CP.

TERCERO. – Esta categoría delictiva se incluye dentro de los delitos económicos, cuya configuración se canaliza a través de una doble fórmula derivada de los perjuicios que pueden causar a través de varias acciones: borrar, deteriorar, alterar, suprimir o hacer inaccesible datos, programas o documentos informáticos (art. 264 CP), obstaculizar o interrumpir el funcionamiento de un sistema informático (art. 264 bis CP), con el añadido de la acción de facilitar la comisión de los delitos precedentes facilitando programas informáticos o contraseñas (art. 264 ter CP).

CUARTO. – Tratándose de delitos económicos y, por ende, de delitos patrimoniales, las acciones descritas en cada uno de los tipos penales deben de estar destinadas a dañar la información o datos que puedan ser cuantificados económicamente. En este sentido, cabe mencionar que los daños que recaen sobre los datos almacenados en un dispositivo informático pueden no contener el elemento económico exigido por la ley y ser igualmente gravosos para el sujeto que lo sufre. Establecer la frontera de la punibilidad en el elemento económico quizás no ha sido lo más acertado ya que elimina de su protección aquellos elementos (entendidos como datos, programas informáticos o documentos electrónicos) contenidos en un sistema informático que no tienen valor económico o que, aún no teniéndolo, podrían tenerlo.

QUINTO. - Resulta fundamental tomar conciencia de la gravedad de estos fenómenos delictivos e incidir en la adopción de una serie de medidas de seguridad informática, ya sea para los dispositivos personales, ya sea para los sistemas empresariales. Si bien hoy en día existen muchas herramientas de protección de la información contenida en los sistemas informáticos, al igual que estas herramientas avanzan, también lo hacen los medios de ataque que consiguen contaminar la información y finalmente hacerse con ella o destruirla por completo. A menudo se recomienda el cambio periódico de las contraseñas del sistema informático o de las propias suscripciones a diversas plataformas que contengan información, el uso de herramientas de protección como los antivirus, o la realización de copias de seguridad como medidas para prevenir estos ataques. Hay que resaltar que en ningún caso el uso de estas medidas de prevención elimina la responsabilidad por la comisión del delito y menos el resultado del mismo.

SEXTO. – Merece especial mención la responsabilidad penal de las personas jurídicas. Si bien su creación es relativamente nueva, pienso que esta nueva figura va más allá de la conexión de la persona jurídica con el derecho punitivo. Podría decirse que a través de los mecanismos de control y supervisión que necesariamente deben de tener las sociedades, además del intento de evitar la comisión de delitos por parte de ésta, se trata de implantar un mecanismo de acción ética en el seno de la persona jurídica que marca tanto las conductas de los trabajadores como la de los propios órganos directivos. La naturaleza jurídico penal del modelo de organización y gestión en relación con el principio de legalidad implica la existencia de una eximente, de modo que estaríamos ante una causa de exclusión de culpabilidad o antijuricidad.

SÉPTIMO. – A la luz del art. 31 bis 2. 2º CP, resulta un tanto confuso que el órgano de supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado en la sociedad sea asimismo un órgano de la propia sociedad con poderes autónomos de iniciativa y de control. El hecho de que se trate de un órgano propio de la sociedad, aun con poderes autónomos, puede implicar una desviación del cumplimiento del propio modelo de prevención implantado. La persona jurídica puede disponer de un modelo de prevención de delitos perfecto y aun así no cumplirlo, pudiendo este caso determinarse otras alternativas como la implantación de un órgano de supervisión con las mismas características, pero externo o independiente de la propia persona jurídica respecto de la cual desarrolla sus actividades.

BIBLIOGRAFÍA

BANACLOCHE PALAO J. "Dilemas de la defensa, principios de oportunidad y responsabilidad penal de las personas jurídicas", en *FGE (coord.* Fiscalia General del Estado*) La responsabilidad penal de las personas jurídicas: Homenaje al Excmo. Sr. D. José Manuel Maza Martín*, Fiscalía General del Estado, Madrid, 2018.

CAMACHO VIZCAÍNO, A. (dir, VVAA), *Tratado de Derecho Penal Económico*, Tirant Lo Blanch, Valencia, 2019.

CARRASCO ANDRINO, M.: "El acceso ilícito a un sistema informático" en ÁLVAREZ GARCÍA, F.J (dir., VVAA), *La adecuación del derecho penal español al ordenamiento de la Unión Europea. La política criminal europea*, Tirant lo Blanch, Valencia, 2009.

CASTRO CORREDOIRA. M. y VÁZQUEZ-PORTOMEÑE SEIJAS, F.: "La reforma de los delitos de daños: arts. 263, 264, 264 bius, 264 ter, 264 quáter, 265, 266.1 y 266.2 CP" en GONZÁLEZ CUSSAC J.L(dir., VVAA), *Comentarios a la Reforma del Código Penal de 2015*, 2ª ed., Tirant lo Blanch, Valencia, 2015.

DE LA MATA BARRANCO, N. J. y HERNÁNDEZ DÍAZ, L.: "El delito de daños informático, una tipificación defectuosa". *Estudios penales y criminológicos*, nº 29, 2009, pág. 326.

FERNÁNDEZ GARCÍA, Mª. Y.:) "Concepto jurídico indeterminado de servicio esencial en la Constitución española". *Revista de Administración Pública*, nº 190, 2006.

FERNÁNDEZ TERUELO, J. G.: "Parámetros interpretativos del modelo español de responsabilidad penal de las personas jurídicas y su prevención a través de un modelo de organización o gestión (compliance). Incluye un análisis de los modelos de responsabilidad penal de las personas jurídicas en México y Ecuador.", Aranzadi Thomson Reuters, Pamplona, 1ª Edición ,2020.

Fiscalía General del Estado, *La responsabilidad penal de las personas jurídicas: Homenaje al Excmo. Sr. D. José Manuel Maza Martín*, 2018,

GONZÁLEZ RUS, J. J.: "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet" en *Delito e informática: algunos aspectos. Cuadernos penales José María Lidón* (VVAA), nº 4, Universidad de Deusto, Bilbao, 2007.

GUTIÉRREZ MAYO, E.: "Delitos informáticos Paso a paso. Análisis detallado de las conductas delictivas más comunes en el entorno informático". Colex Reader, 1ª Edición., 2021.

MUÑOZ CONDE, F.: "Derecho Penal. Parte especial". Tirant lo Blanch, 23ª ed., Valencia, 2021.
RODRÍGUEZ MESA, Mª. J.: "Los delitos de daños. Capítulo XI del Título XIII del CP tras la reforma de la LO 1/2015", Tirant lo Blanch, Valencia, 2017.
SERRANO FERRER, Mª P.: "El reflejo de las nuevas tecnologías en el derecho penal y otros destellos". *Thomson Reuters Aranzadi*, 1ª Edición, 2016.
SERRANO ZARAGOZA O.: "Compliance penal y responsabilidad civil y societaria de los administradores" (coord. RUIZ DE LARA M.), Ed. Wolters Kluwer, Madrid, 2018.

TEXTOS LEGALES

Circular 1/2016, de 22 de enero, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por la Ley Orgánica 1/2015.
Circular 2/2011, de 2 de junio, sobre la reforma del Código Penal por la Ley Orgánica 5/2010 en relación con las organizaciones y grupos criminales.
Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la Ley Orgánica 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos.
Convenio sobre la ciberdelincuencia, Budapest, 23 de noviembre de 2001.
Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005junio, relativa a los sobre ataques contra los sistemas de información.
Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la
Ley 37/2011, de 10 de octubre, de medidas de agilización procesal.
Ley 59/2003, de 19 de diciembre, de firma electrónica.
Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
Real Decreto de 22 de agosto de 1885 por el que se publica el Código de Comercio.
Real Decreto de 24 de julio de 1889 por el que se publica Código civil.

Real decreto Legislativo 1/1995, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital.

Reglamento (UE) 2015/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta el tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Resolución de 19 de julio, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.

ENLACES WEB

ALEGSA (https://www.alegsa.com.ar/). Última conexión: 29.05.2021.

Ciberamenazas y tendencias. Análisis de las ciberamenazas nacionales e internacionales, de su evolución y tendencias. Edición 2021, CCN-CERT (Centro Criptológico Nacional). Disponible en https://www.ccn-cert.cni.es/. Última conexión: 28.03.2022.

Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Seguridad de las Redes y de la Información: propuesta para un enfoque práctico, de 6 de junio de 2001, Bruselas, pág 10. Disponible en: https://eur-lex.europa.eu/. Última conexión: 28.3.2022.

CORCOY BIDASOL, M.: "Protección penal del sabotaje informático. Especial consideración de los delitos de daños." *Diario La Ley*, 1990, nº. 1, 1000-1016. Disponible en: https://diariolaley.laleynext.es, última conexión 21.04.2022.

Desarrollar Inclusión (https://desarrollarinclusion.cilsa.org/). Última conexión. 29.05.2022.

MOIG ALTOZANO M.: "La responsabilidad penal de las personas jurídicas: societas delinquere et puniri potest", *Noticias Jurídicas*, 2012. Recuperado de: https://noticias.juridicas.com/. Última conexión: 19.04.2022.

ÍNDICE JURISPRUDENCIAL

Sentencia de la Audiencia Provincial de Valladolid de 8 de junio, Sección 2ª, n.º 82/2020, (ECLI:ES:APVA:2020:440).

Sentencia del Tribunal Supremo de 16 de marzo, Sala Segunda de lo Penal, n.º 221/2016, (ECLI:ES:TS:2016:966).

Sentencia del Tribunal Supremo de 17 de enero, Sala Segunda, de lo Penal, n.º 30/2001, (ECLI:ES:TS:2001:167).

Sentencia del Tribunal Supremo de 2 de septiembre, Sala Segunda de lo Penal, n.º 514/2015, (ECLI:ES:TS:2015:3813).

Sentencia del Tribunal Supremo de 27 de enero, Sala Segunda, de lo Penal, n.º 97/2004, (ECLI:ES:TS:2004:378).

Sentencia del Tribunal Supremo de 5 de marzo, Sala Segunda, de lo Penal, n.º 232/2012, (ECLI:ES:TS:2012:1844).

Sentencia del Tribunal Supremo de 8 de junio, Pleno de la Sala Segunda, de lo Penal, n.º 154/2016 (RJ\2016\600).