Universidad Internacional de La Rioja
Grado en Derecho

El daño informático

Trabajo fin de grado presentado por:	Eliana Garau
Titulación:	Grado en Derecho
Línea de investigación:	Académica
Director/a:	Dr. Miguel Bustos Rubio

Ciudad
[Seleccionar fecha]
Firmado por: Eliana Garau

CATEGORÍA TESAURO: 3.1 Derecho. 3.1.3 Derecho Público

ÍNDICE

I. LISTADO DE ABREVIATURAS Y SIGLAS

Art: articulo
CP: Código Penal
LECrim: Ley de Enjuiciamiento Criminal
LOPJ: Ley Orgánica del Poder Judicial
L.O: Ley Orgánica
TICs: tecnologías de la información y de la comunicación
Ss: siguientes

EL DAÑO INFORMÁTICO

RESUMEN

El objetivo de este trabajo de fin de grado es realizar un análisis en profundidad sobre el delito de daños informáticos.
En un primer momento analizaremos el contexto socioeconómico y histórico en el cual la intervención del legislador penal para la regulación de esta nueva tipología de daños se hizo necesaria. Del mismo modo analizaremos la normativa vigente á nivel internacional y en España y desde lo general de los delitos informáticos descenderemos hasta los detalles de los conceptos de ajenidad y de sistema informático del articulo 264.2 CP. Como colofón internaremos abordad las posibles regulaciones futuras para así llegar a unas conclusiones personales.

Palabras claves: daño informático, ajenidad, delitos informáticos.

CUMPUTER CRIME

ABSTRACT

The aim of this paper work is to deeply analyse the phenomenon of cyber crime.
On the one hand we will be studying the economical, social and historic contest where the intervention of the legislator was mandatory in order to regulate this new circumstances.

On the other hand we will analyse the current legislation in an International level and in Spain referring in particular to the meaning of non-involvement and to the meaning of informatics system.

The study will follow and we will essay to consider new perspectives and I will discuss my personal opinion.

Key words: cyber crime, non-involvement, informatics crimes.

I. INTRODUCCIÓN

I.1 El origen de la delincuencia informática

Actualmente la colectividad y el entorno social se caracterizan por el fenómeno de la globalización, razón por la cual tanto España como otras naciones se inspiran y se comparan a Estados terceros en el momento de regular determinados nuevos fenómenos potencialmente delictivos.
Los diferentes factores que influyen en la sociedad, como la economía, la cultura, la tecnología se interconectan entre ellos y hacen que los Estados, para poder legislar de forma optímale, no solo tienen que considerar los fenómenos típicos del propio territorio sino que tienen que abrirse a nuevos horizontes y confrontarse a las regulaciones de otros países. Este confronto puede ser, de un lado inspirador para evidenciar los puntos débiles del sistema y de otro lado puede facilitar la identificación de los puntos fuertes de la propia legislación interna. La globalización hace que todas las naciones sean cada vez más cercanas y hace que la influencia entre ellas alcance los niveles más altos.

Sin duda, la tecnología es una de la razones principales que determina la conexión entre los Estados, la susodicha ha experimentado una evolución cósmica en esta ultima década tal que la civilización ha registrado un nivel de conexión que ha permitido un avance de la sociedad a un ritmo inimaginable. Los resultados de lo anterior se detectan fácilmente en la vida de todos los días que se ha hecho mucho más cómoda y práctica.[1]

No obstante todas las ventajas del avance tecnológico, en este magma evolutivo han encontrado espacio también nuevos fenómenos delictivos. Esta evolución tecnológica no ha llevado solo beneficios sino que ha sido también la cuna para que un nuevo tipo penal se desarrollara: el delito informático o “ciberdelito”.[2]
Este tipo penal incluye todas aquellas conductas delictivas que son el resultado de un uso indebido de las nuevas tecnologías. La utilización delictiva de las nuevas tecnologías llega a perjudicar diferentes bienes jurídicos de tal modo que los efectos se presentan y se notan no solo en una dimensión individual sino que también en una dimensión general, a nivel patrimonial y no rigurosamente patrimonial.

Esta reciente organización social se caracteriza por nuevas situaciones de riesgos, nuevos elementos de peligro que tienen que contrastarse con modernas medidas de protección, tanto substanciales como cuantitativas.
En esta novedosa configuración social, definida de riesgo, se ha registrado una aumentación exponencial de las acusaciones de delito informático, que en los últimos tiempos han determinado un numero de detenciones superior a 5000. Asimismo la doctrina ha utilizado esta nueva situación para la creación del “Derecho penal del Risgo” gracias al cual se justifica y se admite la presencia en el territorio nacional de un numero más elevado de fuerzas de seguridad.[3]

---

[1] DOMAICA MAROTO (1997: 9-24).
[2] ANARTE BORRALLO (2001: 121 ss.).
[3] El derecho penal del riesgo ha sido una orientación que se ha desarrollado después de la revolución industrial, en aquella época empezó un numero elevado de actividades que generan riesgos para ellas mismas en relación a factores que no son controlables o lo son muy difícilmente, según esta

El total de denuncias en esta materia llegó hasta las 50,000 lo que testifica una importante diferencia entre los dos datos. El infeliz primado es detenido por el delito de fraude informático.[4] No obstante, tenemos que recordar que en España, los delitos más difusos son los delitos de drogas y de la seguridad vial.
El delito informático, tiene, según las estadísticas, una incidencia mínima en el panorama penal español. ¿Por qué entonces hablar de delitos informáticos? La realidad es que las estadísticas no son capaces de garantizar un imagen fiel a la verdadera situación.[5]

La cifra es relativamente baja porque la mayoría de ciudadanos victimas de delito informático no denuncian, de un lado en consideración de la dificultad de su persecución (los autores de estos delitos tienen, de hecho, la posibilidad de desaparecer dentro del planeta virtual) y de otro lado por el hecho de que no son conscientes de la existencia de este tipo penal. Esta es una de las razones que explica la diferencia entre las personas imputadas, el numero de denuncias y la difusión efectiva del fenómeno criminal.

En este contexto, como hemos adelantado, las estadísticas no reflejan la verdadera realidad.[6] El instituto Nacional de Ciberseguridad, por el medio de una estadística efectuada años atrás, ha demostrado que en la ciberdelincuencia los sujetos pasivos no solo no se identifican como victimas sino que tampoco son conscientes de la repercusión que los susodichos delitos pueden haber en seno a la sociedad, quedan siempre más de impacto, por supuesto, los delitos clásicos contra la integridad física o contra el patrimonio (por ejemplo violencia sexual, hurto etc).

I.2 El legislador español y la delincuencia informática tras los años

El desarrollo de las nuevas tecnologías y, con el paso del tiempo, el desarrollo de los correspondientes abusos han determinado la necesidad que el legislador interviniera para reglamentar algunos fenómenos que estaban empezando a hacer hincapié tanto a nivel internacional como a nivel estatal español.
Muy a menudo la sociedad se desarrolla de manera más rápida respecto a la legislación y así en el ultimo siglo fueron diferentes los peligros originados por las nuevas tecnologías a los cuales el legislador ha intentado dar reglamentación.

La inserción en la sociedad de las primeras tecnologías, absolutamente novedosas para los años 60, fomentó esencialmente unos problemas relacionados con los derechos de la personalidad, de forma que en aquella época la normativa, en diferentes países, se focalizaba en la protección de los datos personales.

En la década siguiente el objetivo principal del legislador fue luchar contra los delitos económicos con contenido informático, asunto que sigue siendo muy actual sin que

---

orientación el derecho penal debe de prevenir estas actividades de riesgo en relación al “peligro abstracto”. Es una posición bastante discutible y que ha suscitado muchas disputas en doctrina.
[4] ALVAREZ (2008: 27-30).
[5] http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24 ec6-b1cc-4451-bd06-50d93c006815
[6] http://www.elmundo.es/navegante/2007/06/20/tecnologia/1182325984.html

se conozcan con exactitud los datos estadísticos sobre los efectos producidos por este tipo de criminalidad.

El centro de atención varió nuevamente en la década de los 80 en relación a los famosos casos de hacking, difusión de videos y piratería de software, espionaje informático. El bum de estos fenómenos fue la clave, el evento necesario para que nuestra sociedad reconociera, sin rémora alguna, la existencia de una criminalidad informática que amenazaba el entorno social. Durante esta década, se debatió (en varios Estados) sobre los problemas procesales-penales que se presentaban en relación con la elevación del numero de las tecnologías de la información y comunicación junto con la comisión de delitos, esto llevó con el paso del tiempo a reformas procesales-penales.
En los años 90 la temática principal de discusión en relación con la criminalidad informática se refirió a la divulgación de elementos antijurídicos en la web como material pornográfico, de instigación a la violencia, de incitación al odio y al racismo etc.

Hoy en día la inclusión de este tipo de contenido dentro del concepto de delitos informáticos sigue siendo objeto de debate, sobre todo en el nuevo contesto de las redes sociales que han resultado ser la cuna ideal para la difusión de este fenómeno. El debate acerca de la utilización exagerada de las nuevas tecnologías informáticas se endereza, a partir de los años 2000, en la utilización de sistemas de seguridad técnicos tales que la criptografía, it security, reglamentación de mandatos y interdicciones dentro de este contesto. Es justamente en este ámbito que se desarrolla la noción de daño informático.

En primer lugar procederemos a dar una definición general de delito informático, en segundo lugar colocaremos estas conductas en el marco internacional y finalmente nos concentrarnos sobre el tipo penal de daño informático así como tipificado en el código penal español, para respetar las exigencias de este trabajo nos concentraremos en el análisis del 264 Código penal español con una breve referencia al articulo 264 bis. [7]

II. LOS DELITOS INFORMÁTICOS

II.1 Características comunes

Antes de proceder con el estudio del tipo penal de daño informático, es oportuno analizar algunas de las características comunes a todos los tipos de delitos informáticos.
El ordenamiento jurídico español considera como informático aquel tipo penal que se lleva a cabo por el medio de un elemento con carácter tecnológico. Podremos incluir un delito en la clasificación de delito informático siempre y cuando su comisión cuente con un elemento tecnológico o informático. De ahí deriva que algunos tipos penales pueden cometerse de forma “normal” y de forma cibernética, por ejemplo los delito de injurias, pueden cometerse de forma “tradicional” y también mediante el uso de las nuevas tecnologías.[8]

[7] DE LA MATA BARRANCO (2009: 311-362).
[8] MIRÓ LLINARES (2014: 423-441).

En el tipo penal de delitos informáticos o ciberdelitos además de los delitos que se ejecutan á través de medios informáticos en sentido estricto como las computadoras o las tecnologías de la información y la comunicación (TICs), se incluyen también aquellos que se ejecutan a través otros medios como smartphons, teléfonos.
En el momento de la comisión de un delito informático serán llamadas en campo dos jurisdicciones, de hecho, la generalidad de delitos informáticos, siendo realizados por medio de la red brindan muchas oportunidades de conectar con las victimas a distancias, muy a menudo victimas que se encuentran en otro País. Esto lleva como consecuencia problemas en relación a la legislación aplicable.[9]

La cuestión es la siguiente: es aplicable la ley de país del autor del delito o la ley del País donde se consuma el delito (país de la victima)? De manera general, la teoría que la doctrina mayoritaria aplica es aquella de la ubicación según la cual se considera tanto el lugar donde se desarrolló la acción delictiva tanto el lugar donde se realizó el efecto, el resultado. En relación a la teoría de la ubicación España sería competente para juzgar estos delitos si fue en su territorio que se produjo el resultado o la actividad antijurídica.

La configuración de la ubicación debe de consagrarse a lo establecido en las normas comunes de territorialidad ex art 23.1 de la LOPJ y los art 14 y ss. De la LECrim.
La situación aquí descrita caracteriza los ciberdelitos siendo la red el principal instrumento que proporciona conexión, de forma instantánea, en cualquier momento y desde cualquier parte del mundo. Aunque podríamos pensar que los autores de esta clase de delitos sean personas con un cierto nivel de conocimiento informático, como hackers o crakers de los cuales muchas veces se entiende hablar en las noticias, puede, y así es en la mayoría de los casos, que los autores del delito sean personas corrientes. Por ejemplo Pepito Peréz que sube en las redes sociales fotos comprometidas de su novia en ausencia de su consentimiento, cometería un delito ex art. 197 CP: violación de la intimidad á través de medios informáticos.
Este no es el caso de los delitos de daños informático que para su ejecución requieren altos niveles de conocimientos técnicos.

Otra peculiaridad de los ciberdelitos es la dificultad no solo de la identificación y de la averiguación de los hechos sino que también de la identificación de los autores que como adelantado en la introducción pueden ocultarse en la red (encriptación, codificación). Es evidente que el uso más frecuente de internet expone a un riesgo más elevado de ser victima de este tipo de delito puesto que en la navegación es frecuente encontrarse en paginas susceptibles de contener virus, troyans u otros tipos de elementos de riesgo.[10]

En conclusión los delitos informáticos constituyen un nuevo tipo penal que hoy en día sigue crescendo cada día más. Por este motivo el Estado se ha adaptado en la manera de oprimir y indagar estos delitos: han sido instituidos nuevos sectores en el Cuerpo Nacional de la Policía[11] y en la Guardia Civil que tienen el único objetivo de perseguir e investigar los susodichos delitos.[12] El código penal español se ha

[9] GONZALES DE CHAVES CALAMITA (2004: 45-66).
[10] ORTS BERENGUER-ROIG TORRES (2001: 44-47).
[11] http://www.policia.es/org_central/judicial/udef/bit_alertas.html
[12] https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

adaptado a la evolución de la criminalidad gracias a su reforma de 2015 y el legislador ha intervenido también a nivel europeo.

II.2 Instrucción del 2/2011 emanada por la Fiscalía General

El Código Penal español no clasifica de ningún modo los delitos informáticos, simplemente se encuentran diseminados en sus diferentes Títulos de la parte especial; la denominación de "delito informático" ha sido introducida en el CP solo con la reforma del 2015.[13]
Con el fin de la identificación y de la clasificación de los susodichos delitos es por lo tanto esencial hacer referencia a la Instrucción del 2/2011 emanada por la Fiscalía General del estado como consecuencia de la creación en el 2010 de un apartado especializado en materia de Criminalidad Informática.[14] Esta instrucción tiene el merito de facilitar la clasificación de los diferentes delitos informáticos con características concretas, lo cual facilita en gran medida la interpretación de la materia. Esta clasificación se hace en consideración de 3 apreciaciones:

- In primis, los delitos cuyo objeto delictivo principal coincide con los sistemas informáticos en si. [15]

- En secundis los delitos cuya acción delictiva aprovecha, para su realización, de las ventajas ofrecidas para las nuevas tecnologías.[16]

- En terzis, se considera la actividad delictiva para cuya realización se necesita, no solo de las TICs (tecnologías de la información y de la comunicación) sino que también de determinados conocimientos técnicos.[17]

No obstante, este listado puede fácilmente alargarse, según la disposición conclusiva de esta instrumentación, de hecho, se pueden incluir todos aquellos delitos cuya realización haya necesitado el uso de las tecnologías de la información y de la comunicación y que este hecho provoque una particular dificultad en el proceso de investigación criminal.

Entre otras cosas la novación del Código Penal LO 2/2015, de 30 de Marzo, ha clasificado y individuados unos tipos concretos de ciberterrorismo. Entre ellos "*el adiestramiento pasivo mediante el uso de las redes de comunicación y tecnlogías de la información y la comunicación*". [18]

En conclusión el cibercrimer es un "sector" en expansión que ha sido provocado por el desarrollo de las nuevas tecnologías. Procedemos ahora a analizar en detalle en primer lugar la normativa a nivel europeo e internacional para luego centrarnos sobre

---

[13] En este sentido, véase el art 127.bis CP
[14] https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/memoria2012_vol1_instru_02.pdf?idF ile=6311c525-d23a-45d7-9e50-458f6f8c3406
[15] En este sentido, véase: delito de daños (art. 264 y ss. CP); el descubrimiento y revelación de secretos contra particulares o empresas (art. 197 y 278 CP); y los delitos contra los servicios de radiodifusión e interactivos (art. 286 CP).
[16] En este sentido, véase: delito de estafa, tecnologías de la información y de la comunicación)
[17] En este sentido, véase: falsificación documental, apología o incitación a la discriminación, crimines de genocidio, delitos de odio y de violencia.
[18] http://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3440.pdf

el delito de daño informático así como regulado en el ordenamiento jurídico español.[19]

III. EL DAÑO INFORMÁTICO

III.1 Perspectiva internacional

La difusión y la importancia de los delitos informáticos ha llevado a la necesaria regulación del fenómeno a nivel supra estatal. Empezamos por lo tanto el análisis de los delitos informáticos en la escena mundial, procediendo a identificar la normativa aplicable a nivel internacional para luego llegar al estudio jurídico-penal especifico del tipo penal nacional. En este apartado nos focalizaremos en la dimensión estrictamente internacional de los susodichos delitos que influencian de forma determinante la regulación penal española.

Los delitos informáticos y así el daño informático encuentran, a nivel supraestatal, su principal reglamentación en el Convenio sobre la Cibercriminalidad de Budapest de 23 de noviembre de 2001[20], es en este contexto que se sientas las fundamentas de una reglamentación penal común, en la mesura de lo posible, al conjunto de los estados signatarios y en la Decisión Marco 2005-222-JAI del Consejo de Europa del 24 de febrero de 2005[21].

Procedemos a analizar en primer lugar el Convenio sobre la Cibercriminalidad de Budapest de 23 de Noviembre 2001. Entre los principales objetivos del texto destacó la necesidad de establecer una regulación imperativa que armonizase las diferentes regulaciones penales de los Estados firmantes. El convenio tiene carácter impositivo y es uno de los principales instrumentos de derecho internacional que tiene como fin la armonización de los delitos derivados de las nuevas tecnologías. Además que los estados miembros de la Unión Europea signaron el susodicho Convenio también Canadá, Sudáfrica, Japón y Estados Unidos de América. Es sin duda la herramienta de derecho internacional penal de delitos informáticos más significativa, no solo por su contenido sino que también por el gran numero de participantes.

Es importante recordar como las disposiciones ratificadas en este Convenio no benefician de una utilización inmediata, su construcción es tal que constituye el principal poder de guiar los Estados en la promulgación de la normativa interna, asi que en el texto nos enfrentamos muchas veces a expresiones de este estilo: “cada parte adoptará las medidas legislativas”. El texto consta de 4 capítulos y en el marco de nuestro estudio será de mayor relevancia el capitulo segundo donde se regulan las prácticas que deben de ser respectadas por los Estados en el momento de la regulación interna del tipo penal y procesal.

España fue uno de los primeros países en firmar, lo ratificó solo el 3 de Junio de 2010, y entró definitivamente en vigor solo el 1 de Octubre del mismo 2010.

---

[19] CAMACHO LOSA (1987: 45).
[20] https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
[21] https://www.boe.es/buscar/doc.php?id=DOUE-L-2005-80503

El Convenio sobre Cibercriminalidad de Budapest analiza los rasgos de los daños informáticos en el artículo 4.1 titulado “atentados contra la integridad de los datos”. El objetivo de este epígrafe es coercer los Estados firmantes a que tomen las iniciativas necesarias para transformar en infracción penal el hecho de provocar un daño, de borrar, de crear un deterioro, una alteración o la supresión de datos, siempre que tal infracción sea no autorizada y voluntaria. Se quiere que los Estados tomen iniciativa para que la misma regulación se obtenga en el derecho interno nacional. Esta disposición despacha protección, en vía directa, exclusivamente a los fundamentos lógicos de los procesos informáticos y incluye aquellas conductas que provocan una modificación del contenido de un dato, en esta disposición no se incluye la destrucción de un objeto. Por elementos lógicos nos referimos al software y la norma no detalla como se tiene que desarrollar el ataque.

En el articulo 5 del mismo Convenio “atentados contra la integridad del sistema”, se analiza la obstaculización grave, realizada con dolo y sin concesión, de la operatividad de un sistema informático, a través de la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos, comportamientos que hacen referencia a las ofensivas de rechazo de servicio o a cualquier otro comportamiento a través del cual, entre otras cosas, se haga imposible el acceso al sistema o se ralentice su funcionamiento.

En relación a nuevos fenómenos de delincuencia informática uno de los fines principales del convenio es solidificar la cooperación entre los Cuerpos Nacionales de Policía de las naciones participantes y armonizar y unificar la normativa penal en materia de lucha contra los ataques a los sistemas de información.[22]

Por otro lado, la Decisión Marco 2005-222-JAI del Consejo de Europa de 24 de Febrero de 2005 se focaliza en los ataques a los sistemas de información.
En su primer articulo la Decisión Marco 2005/222/JAI, del 24 de Febrero, define los “sistemas de información” como “todo apartado o grupo de apartados interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización protección y mantenimiento”.
Estos sistemas de información así definidos deben de ser adoptados por todos los Estados miembros. Por sistema de información se entiende sistema informático.

El articulo 3 rubricado “intromisión en los sistemas de información” se caracteriza por una formulación muy amplia. El texto del articulo 3 dispone que los Estados miembros en el derecho interno deberán sancionar los comportamientos realizados a falta de aprobación que consistan en “obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos”.

[22] TORTRAS (1989: 45).

La disposición incluye de esta forma una gran variedad de comportamientos según los cuales pero no es suficiente una intrusión no legal en la estructura informática sino que también es imprescindible un deterioro a la operatividad del sistema.

Los artículos hacen referencia al ataque a datos o a sistemas y la escritura de la norma hace referencia a cualquier tipo de conducta en que se afecte la integridad o la disponibilidad de los mismos. En particularidad en la Decisión se reenvía también al paradigma de uso seguro, privado, confidencial y libre de obstáculos.
La referencia que nos llega de las normas internacionales tiene que coincidir con la total posibilidad de utilizar un sistema del cual somos legítimos titulares, que permita desarrollarnos en la moderna sociedad según los criterios que consideramos más oportunos.

III.2 Otras fuentes internacionales

En este contexto internacional resultan relevantes las publicaciones de la OCDE[23] y le rol adquirido por la Organización de Naciones Unidas (ONU)[24]. Estas instituciones tienen la difícil tarea de promover una cierta uniformidad en los criterios en el momento de clasificar y identificar los delitos informáticos.

Como en muchas de sus intervenciones los informes de estas entidades carecen de fuerza coercitiva y tienen mero carácter orientativo (esto mismo por ejemplo pasa en materia de convenciones fiscales internacionales), no obstante, la fuerza y la importancia de estos organismos hace que lo aconsejado por ellos tenga una cierta relevancia así que se establecen las primeras herramientas que tienen como objetivo la unificación del nuevo fenómeno delictivo a nivel internacional que comienza a aparecer en la década de los 80.

El 20 y 22 de Noviembre de 1997 se celebran en España, Merida, las Jornadas Internacionales sobre el Delito Cibernético gracias a la coordinación de la UNED (Universidad Nacional de Educación a Distancia de España) y a la sección especializada de la Guarda Civil. En estas Jornadas participaron varios expertos tanto a nivel nacional como internacional, del sector jurídico, político y policial.
Los temas tratados fueros varios, desde el rol de las Fuerzas y Cuerpos de Seguridad del Estado hasta los daños informáticos en concreto.[25] Se sentía la exigencia de reglamentar adecuadamente a nivel penal los comportamientos delictivos determinados por el uso abusivo de las nuevas tecnologías.

La primera regulación de los delitos informáticos a nivel penal se ha registrado en los Estados Unidos que ya tipificaba en los años ochenta el delito de daño informático. En Europa las primeras reglas penales en el ámbito tecnológico se registran en Alemania en 1986.

[23] OCDE: “Guía por la seguridad informática”, 1992: www.oecd.org/internet/interneteconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm
[24] http://www.un.org/fr/index.html
[25] MOLINA-REBOLLO DELGADO-MINGUET MELIÁN (1998: 388-411).

IV. ANALISIS DEL TIPO PENAL DEL DAÑO INFORMÁTICO

IV.1 Análisis del tipo penal

El actual Código Penal español se aprobó por la ley orgánica 10/1995[26], de 23 de noviembre, y introdujo en el ordenamiento jurídico español el delito de daños informáticos que, en su art 264 CP prevé una pena de prisión de uno a tres años y una multa de doce a veinticuatro meses al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Es un clasificación muy genérica que hizo que el legislador incorporase y clasificase el delito con la categoría de daños de propiedad ajena.
Después de más de una década, en conformidad con la Decisión Marco 2005/22/JAI, de 24 de Febrero, relativa a los ataques contra los sistemas de información, el nuevo Código Penal (Ley Orgánica 5/2010, de 22 de Junio) intervino para conformar la regulación de los delitos informáticos al Derecho de la Unión Europea.[27]
Desde aquella fecha se diferencian dos clases de conductas punibles:

1) Por una parte, la nueva formulación del Art. 264 del CP tipifica un numero más elevado de conductas, incluyendo en el tipo penal casi todo tipo de intromisión que interfiera en las plataformas ajenas o en los sistemas externos, presupuesto fundamental es que este tipo de injerencias puedan clasificarse como graves (sentencia de la Audiencia Provincial de Madrid SAP M 8388/2012, de 3 de Junio)[28].
   Aquí el articulo 264 CP dispone que el que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.

   En el apartado numero dos se establece que: “el que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años”.

   El requiso que parece fundamental de la interpretación literal del texto es la gravedad: no solo en las modalidades de la acción sino que también en relación al resultado realizado. Esta interpretación ha sido confirmada en la

[26] https://www.boe.es/buscar/doc.php?id=BOE-A-1995-25444

[27] URBANO CASTRILLO (2012).

[28] http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8119700&links=SECRETO%20EMPRESARIAL%20%22competencia%20desleal%22%20adpic&optimize=20170816&publicinterface=true

sentencia 392/2012, de 4 febrero de la Audiencia Provincial de Asturias[29] supuesto en el cual tres dependientes de una impresas fueron acusados de delito de daños informáticos. La Audiencia explicó claramente como las razones de la absolución han de buscarse en el hecho de que el elemento de gravedad no ha podido individuarse, no solo en el procedimiento sino que también en los resultados realizados, con lo cual el caso concreto no podía reconducirse al tipo penal.

2) Por otra parte, el Art. 197.3 CP estableció que la toma de informaciones sobre datos o programas memorizados en un sistema o en parte de él, en caso de no autorización y en caso de violación de las medidas de seguridad debiesen de ser regulados en el sector del descubrimiento y de la revelación de secretos.

La materia ha subido una nueva renovación en el año 2015 á través de la LO 1/2015 que tipifica el articulo 264 bis, ter y quarter. Por exigencias del trabajo de fin de Grado nos encentraremos en el análisis del art 264 CP con algunas referencias a lo dispuesto por el articulo 264 bis CP.

Procedemos ahora a analizar el tipo penal del articulo 264 del CP, recordando que la categoría de los delitos informáticos es de origen doctrinal y que por lo tanto una clasificación parecida no es presente dentro de la LO, 2015.

IV.2 El bien jurídico protegido

Los artículos 263 y ss CP definen el delito de daños informáticos que se ubica en el Capítulo IX del Título XIII, libro segundo del CP. Cabe destacar que la regulación concreta del delito de daño informático se realiza en los artículos 264 y 264 bis, ter y quarter, novedades añadidas tras la reforma del 2015.

El Título XIII individua una multiplicidad de tipos delictivos que pueden atentar tanto al orden socioeconómico en general como al patrimonio del sujeto pasivo en su singularidad. En relación al bien jurídico protegido hay una discusión doctrinal. Se dice que es pluriofensivo y que se protege el patrimonio en general, el conocimiento, la alcanzabilidad del mismo y la protección de los sistemas informáticos. En la tipificación del tipo penal español han sido de fundamental influencia in primis el Convenio sobre la Ciberdelincuencia realizado en 2001 en Budapest y en secundis la Decisión Marco 2005/222/JAI del Consejo.

IV.3 El daño informático: el tipo objetivo

Nuestro legislador ha decidido no castigar el mero ingreso sin autorización en un sistema informático de un tercero. Es un comportamiento que no integra el tipo penal porque una vez que el sujeto activo se encuentra en el sistema es necesario que ponga en acto ciertas acciones identificadas en el tipo enderezadas al aniquilamiento del objeto material en cuestión. El simple ingreso es exente

[29] https://delitosinformaticos.com/09/2010/noticias/la-audiencia-provincial-de-madrid-absuelve-a-cuatro-imputados-por-un-delito-de-trabajo-falso

penalmente siempre que no vaya junto a actos que tienen como objetivo la producción de daños. El sistema informático está tutelado en relación al software y no en relación al hardware, este último está tutelado por el delito clásico de daños.

El daño informático hace referencia al software, a los elementos lógicos de la parte intangible del sistema. El primer coma del articulo 264 CP establece una previsión de carácter general según la cual: *"El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años".*[30]
El tipo penal considera diferentes comportamientos como borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesible; conductas que impiden el acceso o el utilizo de programas, documentos o datos informáticos.

La pena de prisión por este tipo de delito ha pasado de dos a tres años con la reforma penal de 2015.
Para integrar el tipo penal es necesario que el titular del objeto del delito no hubiese dado su autorización al utilizo y que las consecuencias de esta violación sean graves. La determinación de la gravedad pone varios problemas, sin embargo, como regla general haremos referencia al valor de mercado, tendremos que ver si hay una valoración bursátil, el valor general de la venta y si esto no fuese posible habrá de referirse a una valoración pericial. Para referirse al delito de daño informático a veces se utiliza la expresión sabotaje informático de forma que este tipo penal se distancie aun más de lo establecido en el tipo básico de daños ex art 263 CP.[31]

Bien que el principal bien jurídico protegido en los delitos de daños informáticos sea el patrimonio, podemos individuar, de acuerdo con MUÑOZ CONDE[32], un valor moral del daño siempre que sea susceptible de valoración económica.
En este sentido Muñoz Conde diferencia entre daño sentimental y material afirmando que "*el perjuicio debe ir referido al daño en el objeto material mismo, independientemente de que otros tipos de perjuicios económicos o morales puedan ser tenidos en cuenta para determinar la pena"*.

En el coma dos del articulo 264 CP se individúan 5 circunstancias agravantes.
Las primeras dos ya estaban establecidas en el texto del 2010 mientras que las tres últimas han sido introducidas por la reforma del 2015.[33]
Estas agravantes se caracterizan todas por el hecho de que las conductas tienen como contenido objetos material muy distintos entre ellos que pasan de bienes primarios a bien tutelas por las fuerza de Seguridad Nacional.
No obstante, esto actos delictivos, si realizados en el contexto de una organización terrorista serán calificados como delitos de ciberterrorismo, constituyendo unas conductas que no están subsumidas por el tipo penal de daño o sabotaje informático.[34]

[30] https://vlex.es/tags/articulo-264-codigo-penal-3555446
[31] MARCHENA GOMEZ (2001: 353-366).
[32] MUÑOZ CONDE (2017: 476).
[33] https://vlex.es/tags/articulo-264-codigo-penal-3555446
[34] CORTIJO FERNANDEZ (2013: 614-621).

El tercer coma establece la agravante de la comisión del delito a través de la utilización de datos personales ajenos con el fin de entrar en el sistema informático de un tercero, aprovechándose de la confianza precedentemente ganada gracias a las informaciones personales percibidas de forma ilegal.[35] La agravante solo se integra en el supuesto en el cual los datos personales de terceros fuesen necesarios para la introducción en el sistema dañado o con el fin de ganarse la confianza de este ultimo.

El daño informático es un delito de resultado, el tipo penal se integra siempre y cuando se realice concretamente el resultado descrito en el CP, la mera acción no bastaría. El resultado tiene que ser el fruto de una de las causas señaladas en el tipo penal y el delito puede cometerse activamente o de forma omisiva. No obstante, la comisión por omisión solo se admite en el supuesto de que el autor cubra un rol de garante en relación al bien en cuestión, no sería suficiente para la integración del tipo penal una simple y sencilla omisión.[36] Se configurará delito de daño informático y se integrará el tipo penal solo en el caso de que el sujeto omita la conducta que el legislador español se atiende de el.[37]

Las acciones descritas en el art 264 CP han de ser definitivas, el daño, la alteración de datos, programas o documentos tiene que determinar de forma permanente la no utilización, si así no fuera simplemente la comisión del delito quedaría en grado de tentativa puesto que no ha habido una eliminación total de los elementos claves y que estos pueden ser recuperados o instalados otra vez.
El delito se queda en grado de tentativa también en el supuesto en el cual el resultado no se realice por motivos ajenos a la voluntad del presunto sujeto activo.[38]

IV.4 El tipo subjetivo

En relación al tipo subjetivo el daño informático es un delito doloso tanto en la forma de dolo directo como en la forma de dolo eventual. En necesaria la voluntariedad en la destrucción de los elementos lógicos y físicos del la estructura digital.
En el caso de dolo eventual es necesario que el resultado supere lo que supuestamente el sujeto se esperaba, por ejemplo Pepito Peréz que crea un virus dañoso sin poder determinar si hará daño o si permanecerá “escondido” sin que se produzca algún resultado, no dependiendo de el desarrollo del resultado.

Es aceptada la comisión del delito de daños informáticos de forma imprudente en el caso del deterioro de datos o sistemas por el medio de un comportamiento negligente, posibilidad regulada en el articulo 267 CP que incluye los daños causados por imprudencia grave, en el caso de que los daños amonten a un valor de al menos 80.000 euros. En este supuesto es imprescindible la denuncia del sujeto afectado o de su abogado, se admite también la denuncia por parte del Ministerio Fiscal si la victima es menor de edad, con discapacidad o que necesite de especial cuidado u protección. El presunto autor del delito será persona física o jurídica según

[35] En este sentido, véase art 197 CP como agravante estrictamente conectada con los delitos de la intimidad
[36] A titulo de ejemplo consideren el programador informático de una empresa que no impida el desmantelamiendo del sistema del caul es garante por parte de un virus informático.
[37] BOIX REIG (2016: 44).
[38] SOLER ARESPACOCHAGA (1995: 9-24).

los casos y en concreto el articulo 264 quarter regula el delito de daño informático cometido por una persona jurídica. Entre las novedades de la reforma del 2015 se incluye un articulo que define el caso en el cual las conductas contempladas en los apartados anteriores sean cometidas por parte de una persona jurídica, en calidad de sujeto activo de delito.[39] El resultado de la reforma parece aportar una estructura más clara y más sencilla.

IV.5 Autoría y participación

En relación a las modalidades de autoría, participación y actos preparatorios la regulación penal se ajusta a los principios generales del mismo CP.
En este contexto nos enfrentamos fácilmente a la autoría mediata que suele ser la forma más común de comisión del hecho delictivo.

La autoría del delito de daños informáticos releva de una peculiaridad en relación a los otros tipos de delitos informáticos porque solo puede realizarse por personas que tengan conocimientos específicos de la red. Como ya hemos adelantado antes, esta es una característica que no pertenece a todos los ciberdelitos (injurias, amenazas, difamación donde es suficiente el mero acceso a Internet a través, por ejemplo, de un social network). Para la ejecución del delito de sabotaje informático el sujeto activo debe de tener unos ciertos conocimientos de la ciencia informática.

Asimismo podemos individuar una clasificación tripartida en relación a la autoría:
a) los hackers, aquellas personas que sin permiso consiguen el ingreso a computadoras o sistemas informáticos, usualmente tramite líneas telefónicas publicas, sin la intención de provocar un daño. El objetivo final en general se identifica en el menoscabo de la intimidad del sujeto pasivo o en el otorgamiento de una precisa indicación que todavía no se quiere destruir.

Dentro de la categoría de los hackers podemos individuar los hackers blancos que tienen como objetivo la protección de las TICs, suelen ser o salariados de empresas de seguridad informática o simplemente expertos informáticos que por entretenimiento se consagran a eliminar las barreras de lo sistemas, sin intención de ocasionar ningún perjuicio, puesto que se trata de hackers blancos.

b) los crakers, aquellos que precisamente dañan los sistemas informáticos a través del ingreso o la contaminación de estos. Los crackers tienen intención de dañar, entran en los sistemas con la intención de provocar un daño: por ejemplo eliminar o borrar ficheros o asimismo introducir específicos tipos de virus. Esta es la figura típica de autoría del 264 y ss. puesto que se registra la especifica voluntad de dañar, borrar, eliminar etc, así como previsto por la letra del articulo. [40]

c) Los sniffers, se introducen en los sistemas informáticos con el fin de obtener determinados conocimientos. El modus operandi lleva el nombre de sniffing y es aquella práctica que examina todos los paquetes informativos que pasan por una red, de modo que los sniffers los abren y captan las informaciones necesarias (contraseña por ejemplo) para poder realizar futuras actividades. [41]

[39] https://www.abogacia.es/2015/03/09/analisis-juridico-del-sabotaje-informatico/
[40] http://hackersycrackers-yi.blogspot.com/
[41] ROMEO CASABONA (2006: 241-271).

Una vez que el sujeto activo se ha introducido en el sistema informático ajeno tiene básicamente dos opciones. De un lado el bloqueo o la inutilización de las websites o en general de los servicios de internet, eso puede tener carácter temporal o definitivo y puede ser parcial o total, o, de otro lado, la alteración o la destrucción, general o individual del objeto como informaciones o datos de terceros.

Las dos situaciones son consideradas por el legislador penal español porque, en todo caso lo que tiene relevancia jurídica es el daño causado y su gravedad.
El resultado de dañar puede realizarse de diferentes formas con diferentes tipos de acciones por ejemplo a través el establecimiento en el sistema de gusanos, bombas lógicas, virus, troyanos, bacterias o otros elementos potencialmente dañinos de los sistemas informáticos. Recordamos que siempre tiene que tratarse de perjuicios definitivos a los cuales no se puede poner remedio con una simple reinstalación, también se incluyen en este tipo penal la remesa de mensajes falsos o en numero tan elevado que provocan el colapso del sistema. A esta práctica tiene que seguir la inutilización total del sistema. [42]

IV.6 Concepto de ajenidad y de patrimonio: art. 264 CP

Las interpretaciones en relación al art 264.2 CP son esencialmente dos: una primera hace referencia a la ubicación del dictado normativo y lo considera como una modalidad cualificada del tipo básico de daños. En relación a esta primera interpretación el delito de daños informáticos deberá integrar no solo los elementos regulados en el tipo cualificado sino que también los elementos del tipo básico.
Una segunda interpretación considera el daño informático como una modalidad especifica porque en realidad en este caso el texto normativo no hace referencia a los daños individuados en el precedente articulo (art. 263 CP).

La consideración del delito de daños como infracción de carácter patrimonial es pacifica. No obstante, una parte de la doctrina es de aviso que el tipo básico de delito de daños informático debería disciplinarse en un articulo ubicado en una sección diferente respecto a la de los daños en general. Este delito nació en 1995 como una modalidad autónoma de daños y no como un subtipo del tipo básico del delito de daños.
La opiniones contrastantes y la ideas divergentes en doctrina son un clásico y no son ninguna novedad así que un numero importante de autores considera que la dicha localización debe de considerarse oportuna puesto que nos encontramos frente a un subtipo agravado de delitos de daño.[43]
El legislador ha clarificado las dudas al respecto y nos obliga a entender el delito de daños informáticos como un tipo autónomo agravado y no como un tipo cualificado.

Clarificada la cualificación jurídica del delito ¿que es lo que se pretende verdaderamente proteger a través del significado propio de las palabras del art. 264.2 CP? ¿Que es lo que se debe entender por menoscabo del correcto funcionamiento de los elementos lógicos de un sistema informático? ¿Como debe de interpretarse a la luz de la normativa internacional?

[42] GONZÁLES HURTADO (2013: 327-351).
[43] CORCOY BIDASOLO (1990: 1000).

La doctrina mayoritaria ha considerado y ha llegado a la conclusión que el bien jurídico protegido ex art 264.2 está estrictamente ligado a la idea de propiedad ajena. Lo que se sanciona, de hecho, son los comportamientos dañosos en relación a objetos materiales de dominio ajeno. La letra del articulo define como ajenos los documentos, los programas o los datos que son objeto de la ofensiva, del ataque. Otra consideración que salta a la vista es que la formulación del precepto ex art 264.2 no tiene rasgos en común con el resto de tipos agravados tipificados en el primer apartado del art. 264.

Nuestro objetivo es intentar explicar la relación del contenido del bien jurídico protegido en el delito de daños en relación al concepto de propiedad ajena. En las diferentes posibilidades de relación una parte de la doctrina considera que podría efectivamente encontrarse una persona titular de un derecho de dominio sobre el hardware en el cual se localicen las informaciones atacadas y también, en algunas ocasiones, derechos de propiedad intelectual en relación a bases de datos o programas sobre datos incluidos en el sistema.

Esto implicaría que no podría plantearse la posibilidad de hablar de daños sobre la propiedad ajena porque no seria posible considerarlo como victima de delito de daños. No obstante, no hay que olvidar que en los delitos patrimoniales es suficiente verificar la ajenidad de la cosa para considerar el tipo pertinente, no es necesario demonstrar el titulo sobre la cosa.

Otra parte de la doctrina opina que lo que se quiere proteger en realidad son intereses de contenido económico y que por lo tanto no es necesario hacer referencia al patrimonio en su significado más rígido.[44]
En estos casos y bajo estas consideraciones los efectos económicos más importantes no se circunscriben a la disminución del valor económico de los elementos perjudicados sino que se extended, por ejemplo, a la afectación de la actividad empresaria que se esté realizando. Esto se podría examinar en sede de responsabilidad civil.

Estos tipos de inconvenientes relacionados col considerar el bien jurídico protegido el patrimonio o intereses de carácter socioeconómico ha animado nuevas ideas que individúan y consideran objeto de tutela el conocimiento de los datos informático y el acceso al los mismos. Lo que asume relevancia desde esta perspectiva es la información, la protección de los sistemas informáticos que debe entenderse como la certeza de no ser victimas de intrusiones ajenas en datos, sistemas informáticos o programas. Estos tienen una importancia extrema para el correcto desarrollo de las nuevas tecnologías que permiten, a través de redes telemáticas independientes, la comunicación pacifica. Es necesario garantizar y tutelar los bienes jurídicos que juegan alrededor de estas actividades: intimidad, protección de datos de carácter personal, estimación del correcto funcionamiento de los sistemas informáticos.

Estos son intereses que relevan no solo desde un punto de vista individual sino que también desde una perspectiva supraindividual en relación a actividades tanto privadas como publicas. Se puede hablar de forma general de la protección del bien jurídico de la tecnología de Internet que incluye muchísimas nuevas implicaciones y actividades no solo personales sino también económicas. En este contexto asume

[44] FERREYROS SOTOS (1996: 470).

importancia el fenómeno de las TICs en todos los sectores, tanto públicos como privados. La sociedad moderna es cada día más ligada al correcto funcionamiento de las tecnologías, desde el bloqueo de un sistema no solo puede subir efectos negativos la vida personal y profesional de una persona, sino que también puede depender el correcto funcionamiento de una empresa hasta llegar al correcto funcionamiento de los sistemas de Seguridad social y de Policía.[45]

La cuestión que tenemos que abarcar ahora es la siguiente: se trata de despachar tutela a la propiedad (bien considerada desde una perspectiva funcional) o se trata de proteger algo que vas más allá de la sola propiedad? El objeto de protección son los datos, documentos o programas almacenados en sistemas informáticos así como establecido tanto por el legislador nacional como por las Instancias internacionales.

Resulta necesario alejarse y no limitarse a la clásica idea de daños identificada en destrucción de un ente, cosa u objeto (o incluso también las consideraciones de daño en relación a la desaparición o a la perdida de utilidad o valor) porque lo que tiene relevancia es la posibilidad de alcanzar tales datos, que estos puedan ser utilizados de modo integro en cualquier momento. No es relevante que su importancia teórica quede intacta, a nada serviría que un dato siga existiendo en alguna parte de la nube si no es posible acceder a eso. [46]

El objeto de la protección tiene que ser la posibilidad de acceder en todo momento a los datos que tienen que conservarse en su integridad.
La razón por cual se presta tutela a la información contenida en soportes informáticos no deriva de la consideración de que esta tenga más importancia que otra información incluida en otros soportes, la clave de esta protección reside en el hecho de que esta información dependen todos los sectores públicos y privados y esto va más lejos que el daño individual al dato o al sistema concreto.[47]

V. EL ARTICULO 264 BIS

La reforma del 2015 introduce el articulo 264 bis que reglamenta el daño al sistema informático en su totalidad, no al dato individual, programa o documento que se mantiene como objeto material del tipo básico del art 264.1 sino simplemente el sistema informático en su conjunto.

Así se destaca de manera más cristalina el contenido material del delito respeto a su antigua formulación. La reforma establecida por la LO 1/2015 establece en su art. 264 un amparo básico en este ámbito, en relación a los comportamientos que atenten contra datos, programas o documentos electrónicos, agravados en determinadas condiciones, mientras que el art 264 bis se ubica aisladamente con respecto al precedente articulo y concede amparo a un objeto diferente y más vasto que se relaciona al tipo básico en el momento en el cual deriva de la letra a)

[45] SALOM CLOTER (2004: 292-318).
[46] MATA MARTIN (2001: 33).
[47] DE LA MATA BARRANCO (2009: 300).

vinculada a las actitudes ex art. 264.1 relacionadas al dañado, deterioro, alterado o supresión, en relación a otro objeto que en este caso es el sistema informático.[48]

Como en el tipo básico ex art. 264 el resultado tiene que ser grave en referencia al valor o patrimonio del sistema y es necesario que el sujeto activo lleve a cabo la acción delictiva sin el previo consentimiento del titular de la propiedad del equipo. Los requerimientos son idénticos a aquellos individuadas en el precedente apartado. Cuando el sistema informático dañado pertenece a una empresa, negocio o a una Administración pública el articulo 264 bis establece una agravante en consideración del mayor perjudico ligado a unas consecuencias económicas de mayor importancias pudiendo perturbar las actividades productivas de las susodichas actividades.

Es indispensable que objeto del delito sea el sistema y no el dato, programa informático o documento electrónico del tipo básico, puesto que la norma solo hace referencia al conjunto del sistema que provoca el verdadero perjuicio a la Administración o empresa, tiene que destacarse la consideración de la forma en su totalidad y no es su individualidad como hecho por la norma básica.

El articulo 264 bis en sus dos últimos apartados reproduce la estructura utilizada en el art 264 en relación a las agravantes.[49]
Constante en la letra de la norma es la distinción entre los datos, programas y documentos electrónicos de un lado y el sistema informático en su totalidad por otro lado. El articulo 264 bis, establecido exclusivamente para la protección de los sistemas informáticos en su conjunto, se remite al tipo básico para las cinco agravantes, del mismo modo a la otra circunstancia agravante referida al conseguimiento de datos personales ex art 197.2 CP.
Las conductas tipificadas en los artículos 264 y 264 bis se diferencian exclusivamente en el objeto material. En su conjunto las dos normas garantizan una protección muy amplia en relación a todo tipo de daño informático.

¿Por qué esta necesidad del legislador penal español? Estos artículos no hacen referencia a la forma de llevar a cabo la realización del delito, solo se considera el resultado: la destrucción, la alteración o inutilización de los datos, programas, documentos electrónicos o sistemas informáticos.

A estas alturas debería resultar claro que el objeto material de los daños informáticos se identifica en las nuevas tecnologías, en detalle los datos informáticos, los programas informáticos, los documentos electrónicos y el tipo agravado de protección al sistema informático ajeno de forma conjunta.

Para llevar a cabo este resultado el sujeto activo tiene múltiples posibilidades de acción que hemos analizado en el apartado IV.5.

[48] https://juiciopenal.com/delitos/danos/delito-danos-informaticos-producido-trabajadores-extrabajadores-una-empresa/
[49] https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565

CONCLUSIONES Y PERSPECTIVAS FUTURAS

Como colofón de este estudio intentaré llegar a unas conclusiones y expresar mi opinión personal.

In primis, el delito informático ha caracterizado el siglo XXI: es un delito que puede determinar la perdida de cantidades ingentes de dinero en poco tiempo y que puede afectar la intimidad de los ciudadanos sin que los susodichos realicen la existencia de una violación.

In secundis, hay que evidenciar como los delitos que han caracterizado el siglo XXI avanzan, se adaptan y se desarrollan en diferentes formas conformemente al avance tecnológico. A nivel mundial existe un gran interés por luchar y contrastar este tipo de conductas, interés que se refleja en la intervención del legislador a nivel internacional. Es deseable que la normativa internacional se caracterizarse por su efectividad y por su dinamismo, elementos que definen las nuevas tecnologías, origen del fenómeno delictivo.

In terzis, es fundamental que las personas victimas de estos abusos tomen conciencia de la existencia de estos fenómenos y que de consecuencia se organicen para protegerse, por ejemplo la aplicación de modalidades de seguridad informática tanto en los sistemas empresariales como en los sistemas domésticos con el fin de prevenir el sufrimiento de las consecuencia de estas acciones ilegales. Los delitos informáticos más comunes son los de daño o sabotaje informático, tema que ha sido central en el avance de este trabajo. Entre los más comunes incluimos los sabotajes a empresas, el uso fraudulento de internet, la fuga de información y el espionaje informático.

Por último, potencialmente los delitos informáticos son infinitos ¿Cuales las perspectivas futuras entonces?

Tenemos que tener mucho cuidado con el manejo de la información que utilizamos de forma sistemática, protegiéndola siempre con claves que habrá de cambiar con frecuencia. Probablemente este es un fenómeno que se ha difundido por faltas de oportunidades, una manera fácil de ganar dinero en un contexto de fuerte crisis tanto económica como moral.
Sería deseable que se estableciera una normatividad global, fortaleciendo les leyes para que sean efectivas, al día y no obsoletas, como impuesto por las nuevas tecnologías.

BIBLIOGRAFÍA:

- ALVAREZ, J.A. (2008), *Análisis forense informático: el delito informático,* Madrid, Mundo Linux, págs. 27-30.
- ANARTE BORRALLO, E. (2001), *Incidencia de las Nuevas Tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información*, Huelva, Universidad de Huelva, págs.12 y ss.
- BARREIRO, J. (1983), *El delito de daños en el Código penal español*, anuario de derecho penal y ciencias penales, págs. 505-532.
- BOIX REIG, F.J. (2016), *Derecho Penal. Parte especial*, España, Iustel.
- CAMACHO LOSA, L. (1987), *El delito informático,* Madrid, Conde de Peñalver, págs. 45-46.
- CORCOY BIDASOLO, M. (2007), *Problemas de la persecución penal de los denominados delitos informáticos*, Eguzkilore, Aquilafuente, págs. 1-33.
- CORCOY BIDASOLO, M. (1990) *Protección penal del sabotaje informático,* Madrid, La Ley revista jurídica española de doctrina, jurisprudencia y bibliografía, págs. 1000-1016.
- CORTIJO FERNANDEZ, B. (2013), *Dirección y gestión de seguridad*, Salamanca, Ciencias de la seguridad, págs. 614-621.
- DE LA MATA BARRANCO, N.J. (2009), *El delito de daños informáticos, una tipificación defectuosa,* País Vasco, Universidad del País Vasco, págs. 311-362.
- DOMAICA MAROTO, J.M. (1997), *El control de riesgos en fraudes informáticos,* Madrid, Fundación Mapfre, págs. 9-24.
- FERREYROS SOTOS, C. (1996), *Aspectos metodológicos del delito informático,* Informática y derecho: Revista iberoamericana de derecho informático, págs. 407-413.
- GIMÉNEZ GARCÍA, J. (2006), *Delito e informática. Algunos aspectosde derecho penal material*, País Vasco, Eguzkilore, págs.197-216.
- GONZALES DE CHAVES CALAMITA, M.E. (2004), *El llamado delito informático,* Madrid, Universidad Complutense de Madrid, págs. 45-66.
- GONZÁLES HURTADO, F. (2013), *Daños informáticos del articulo 264 del Código Penal y propuesta de reforma,* Madrid, Universidad Complutense de Madrid, págs. 327-351.
- MARCHENA GOMEZ, M. (2001), *El sabotaje informático entre los delitos de daños y desórdenes públicos,* Madrid, Cuadernos de Derecho Judicial, págs. 353-366.
- MATA Y MARTIN, R.M. (2001), *Delincuencia informática y derecho penal,* Madrid, Edisofer, págs. 33-34.
- MIRÓ LLINARES, F. (2014), *Cibercrimen y vida diaria en el mundo 2.0. Las teorías del crimen y la oportunidad en ámbitos específicos,* Madrid, Marcial Pons Ediciones Jurídicas y Sociales, págs.423-441.
- MOLINA, J.M.- REBOLLO DELGADO, L.- MINGUET MELIÁN, J.M. (1998), *Informática y derecho: Revista Iberoamericana de derecho informático, ejemplar dedicado a Jornadas internacionales sobre el Delito Cibernético*, págs. 388-411.
- MUÑOZ CONDE. (2017), *Derecho Penal. Parte especial*, Madrid, Tirant lo Blanch, págs. 475-476.

- ORTS BEREBGUER, E. - ROIG TORRES, M. (2001), *Delitos informáticos y delitos comunes a través de la informática*, Madrid, Tirant Lo Blanch, págs. 44-47.
- ROMEO CASABONA, C.M. (2006), *El cibercrimen*, España, Editorial Comares, págs. 241-271.
- ROMEO CASABONA, C. M. (2006), *De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal*,*en El cibercrimen: nuevos retos jurídico-penalesnuevas respuestas político-criminales*, Granada, págs. 1-42.
- ROMEO CASABONA, C.M. (2006), *Los datos de carácter personal como bienes jurídicos penalmente protegidos*, *en El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, Editorial Comares, págs. 167-190.
- ROVIRA DEL CANTO. (2002), *Delincuencia informática y fraudes informáticos*, Granada, Editoriales Comares, pp. 226 y ss.
- SALOM CLOTER, J. (2004), *Aproximación al delito informático y su investigación,* Santiago de Compostela, Defensa e Internet, págs. 292-318.
- SÁNCHEZ GARCÍA DE PAZ. (2002), *Problemas de derecho penal internacional en la persecución de delitos cometidos a través de Interne*, Valladolid, Actualidad Penal, págs. 107-172.
- SOLER ARESPACOCHAGA, J.A. (1995), *El delito informático*, Madrid, Gerencia de riesgos y seguros, págs. 9-24.
- TORTRAS, C. (1989), *Informática y derecho*, Madrid, Icade, págs. 45-50.
- URBANO CASTRILLO. (2012), *Los delitos informáticos tras la reforma del CP de 2010 en Delincuencia informática. Tiempos de cautela y amparo,* 1ª edición Ed, Navarra, Thomson Reuters Aranzadi, págs. 1-15.

DIRECCIONES WEB:

- https://www.abogacia.es/2015/03/09/analisis-juridico-del-sabotaje-informatico/ fecha de última consultación 16.10.2018
- https://www.boe.es/buscar/doc.php?id=DOUE-L-2005-80503 fecha de última consultación 15.12.2018
- Art 264 bis CP https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565, fecha de última consultación 15.10.2018
- Ley orgánica 10/1995 https://www.boe.es/buscar/doc.php?id=BOE-A-1995-25444 fecha de ultima consultación 28.12.2018
- http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t13.htmll fecha de última consultación 17.12.2018
- https://dialnet.unirioja.es/buscar/documentos?querysDismax.DOCUMENTAL_TODO=da%C3%B1os+informaticos+&inicio=21 fecha de última consultación 17.12.2018
- https://dialnet.unirioja.es/buscar/documentos?querysDismax.DOCUMENTAL_TODO=da%C3%B1os+informaticos+&inicio=201 fecha de última consultación 18.12.2018
- https://delitosinformaticos.com/09/2010/noticias/la-audiencia-provincial-de-madrid-absuelve-a-cuatro-imputados-por-un-delito-de-trabajo-falso fecha de última consultación 21.12.2018

- https://dialnet.unirioja.es/servlet/articulo?codigo=75376 fecha de última consultación 27.12.2018
- https://digitum.um.es/xmlui/handle/10201/35511 fecha de última consultación 28.12.2017
- http://hackersycrackers-yi.blogspot.com/ fecha de última consultación 28.12.2018
- https://juiciopenal.com/delitos/danos/delito-danos-informaticos-producido-trabajadores-extrabajadores-una-empresa/ fecha de última consultación 20.12.2018
- http://www.elmundo.es/navegante/2007/06/20/tecnologia/1182325984.html fecha de última consultación 23.12.2018
- https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/memoria2012_vol1_instru_02.pdf?idF ile=6311c525-d23a-45d7-9e50-458f6f8c3406 fecha de última consultación 16.12.2018
- https://www.gdt.guardiacivil.es/webgdt/home_alerta.php fecha de última consultación 16.12.2018
- http://www.interior.gob.es/documents/10180/1207668/Avance+datos+cibercriminalidad+2013.pdf/5de24 ec6-b1cc-4451-bd06-50d93c006815 fecha de última consultación 28.01.2019
- http://www.un.org/fr/index.html fecha de última consultación 22.01.2019
- www.oecd.org/internet/interneteconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm fecha de ultima consulta 27.01.2019
- https://www.oas.org/juridico/english/cyb_pry_convenio.pdf fecha de última consultación 23.09.2018
- http://www.policia.es/org_central/judicial/udef/bit_alertas.html fecha de última consultación 22.10.2018
- http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8119700&links=SECRETO%20EMPRESARIAL%20%22competencia%20desleal%22%20adpic&optimize=20170816&publicinterface=true fecha de última consultación 22.12.2018
- http://roderic.uv.es/handle/10550/63912 fecha de última consultación 22.12.2018
- https://vlex.es/tags/articulo-264-codigo-penal-3555446 fecha de última consultación 15.12.2018