UNIVERSIDAD
INTERNACIONAL
DE LA RIOJA

Universidad Internacional de La Rioja
Grado en Derecho

Ransomware, hacking y phishing: conducta típica del delito de daños informáticos.

Trabajo fin de grado presentado por: Francisco José Balboa Romero
Titulación: Grado en Derecho
Línea de investigación: Derecho Penal
Director: Dr. Francisco José Rodríguez Almirón

Elda
17 de junio de 2018
Firmado por: Francisco J. Balboa Romero

CATEGORÍA TESAURO: 3.1.3 Derecho Público. Derecho penal.

ÍNDICE

LISTADO DE ABREVIATURAS Y SIGLAS 3

RESUMEN 4

I. INTRODUCCIÓN 5

I.1. Antecedentes 5
I.2. Objetivos 6
I.3. Metodología 7
I.4. Agradecimientos 7

II. DEFINICIÓN Y ANTECEDENTES DE LAS CONDUCTAS DE HACKING Y PHISHING. 7

II.1. Definición de los ciberdelitos de hacking, phishing. 7
II.2. El ransomware y el ciberataque del gusano Wannacry de 12 de mayo de 2017. 9
II.2.1. Definición de ransomware. 9
II.2.2. El ataque del gusano Wannacry 9

III. EL DELITO DE DAÑOS INFORMÁTICOS. EVOLUCIÓN Y MARCO NORMATIVO 11

III.1. Convenio Europeo sobre Ciberdelincuencia de 2001 11
III.2. Normativa europea: Decisión Marco 2005/222 y Directiva UE 2013/40. 11
III.3. Concepto y definición de daños informáticos. 12
III.4. Las reformas del Código Penal de 2010 y 2015 13

IV. ANÁLISIS DEL TIPO PENAL DEL DELITO DE DAÑOS INFORMÁTICOS EN NUESTRO SISTEMA PENAL. 16

IV.1. Análisis del bien jurídico protegido. 16
IV.2. El tipo objetivo. 17
IV.2.1. Sujetos activos. 17
IV.2.2. Sujetos pasivos. 18
IV.2.3. Conducta típica. 19
IV.2.4. Objeto material. 22
IV.3. El tipo subjetivo. 23
IV.4. La exclusión de la Antijuricidad. 25
IV.5. Culpabilidad. 26
IV.6. Iter criminis 28
IV.7. Autoría y participación 28
IV.7.1. La problemática de los sujetos activos en la autoría del ataque. 29
IV.7.2. La problemática de la aplicación del Principio de Territorialidad y el tiempo de las conductas delictivas. 30
IV.8. Las consecuencias jurídicas derivadas del delito: Punibilidad. 31
IV.9. La prescripción de los delitos y penas. 33
IV.10. Concursos. 33

V. CONCLUSIONES 35

VI. BIBLIOGRAFÍA Y WEBGRAFÍA 38

VII. FUENTES NORMATIVAS Y JURISPRUDENCIALES 39

LISTADO DE ABREVIATURAS Y SIGLAS

AN: Audiencia Nacional

AP: Audiencia Provincial

Art.: Artículo

CE: Constitución Española

CCN-CERT: Centro Criptológico Nacional

CP: Código Penal

LECrim: Ley de Enjuiciamiento Criminal

LO: Ley Orgánica

ONU: Organización de las Naciones Unidas

Pág.: Página

RAE: Real Academia Española de la Lengua

SS.: Siguientes

SAN: Sentencia de la Audiencia Nacional

SAP: Sentencia de la Audiencia Provincial

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea

STC: Sentencia del Tribunal Constitucional

STS: Sentencia del Tribunal Supremo

TIC: Tecnologías de la Información y Comunicación

UE: Unión Europea

RESUMEN

Los denominados ciberdelitos son una nueva forma de delincuencia y, uno de los grandes retos a los que el derecho debe dar respuesta en el siglo XXI. Las empresas han sido las tradicionales víctimas de esta modalidad criminal, no solo por el uso de las tecnologías sino también por sus recursos económicos, objeto de deseo por los cibercriminales. Además, cualquiera de nosotros, como ciudadanos que nos conectamos en internet, podemos ser objeto de un ciberataque personal.

En el presente trabajo, analizamos los problemas jurídicos de los diferentes tipos penales asociados a los daños informáticos, atendiendo no sólo al perfil individual y colectivo de los delincuentes, los hackers y los crackers, sino también a los problemas de persecución y anonimato que plantean. Las dificultades que se plantean y los posibles retos necesitados de atención por el legislador, se desarrollan desde una visión jurídica del fenómeno, teniendo en cuenta los recientes cambios operados en el Código Penal español.

Palabras clave: ciberdelito, hackear, daños informáticos, intrusión, ataque informático.

ABSTRACT

The so-called cybercrimes are a new form of crime and one of the great challenges to which the law must respond in the 21st century. The companies have been the traditional victims of this criminal modality, not only because of the use of technologies but also because of their economic resources, object of desire for cybercriminals. In addition, any of us, as citizens who connect on the Internet, can be subject to a personal cyberattack.

On this dissertation, we analyze the legal problems of the different criminal types associated with computer damage, taking into account not only the individual and collective profile of the criminals, hackers and crackers, but also the problems of persecution and anonymity that they pose. The difficulties that arise and the possible challenges needed for attention by the legislator, are developed from a legal view of the phenomenon, taking into account the recent changes in the Spanish Penal Code.

Key words: cybercrime, hacking, computer damage, intrusion, computer attack.

I. INTRODUCCIÓN

I.1. Antecedentes

Las nuevas tecnologías han supuesto, como algunos han definido, la tercera revolución industrial, un nuevo paradigma social y cultural, donde diferentes facetas de la vida se interconectan de un modo totalmente distinto a como lo veníamos haciendo hasta no hace más de 10 años. Utilizamos las Tecnologías de la Información y la Comunicación (TICs) para interrelacionarnos con administraciones públicas, con entidades financieras, con familiares y amigos, con los stakeholders en el ámbito de la empresa, etc., y todo ello bajo un modelo de comunicación global. Esta evolución digital ha supuesto a su vez que tengamos una visión distinta y mucho más amplia del Derecho, y con ella, la necesidad de introducir determinados delitos o la modificación de otros existentes en nuestro Código Penal (en adelante CP) ya que los delitos clásicos han evolucionado al igual que lo han hecho los aspectos de nuestras formas de convivencia, obligando al legislador a definir nuevas conductas y formas delictivas.

Esta concepción de algunos tipos delictivos, viene dada por el uso de dichas tecnologías en red, que, si bien han impulsado la transformación digital, no resultan una cuestión baladí, sino que a la vez han tenido un aspecto negativo y es que, a modo de ejemplo, cabe significar que, según el Centro Criptológico Nacional, numerosas pequeñas y medianas empresas fueron objeto de algún tipo de ciberataque en 2016, año en el que se produjeron 113 millones de ataques cibernéticos a nivel mundial, que sirvieron a su vez, en muchos casos, para llevar a cabo accesos no autorizados a sus sistemas informáticos (en inglés, hacking) o sustitución de la identidad con acceso a las contraseñas y estafas utilizando medios informáticos (en inglés, phishing). Y como referencia más cercana prestaremos especial atención, así como objeto de análisis, al ataque informático global producido el 12 de mayo de 2017 mediante el virus[1] informático de tipo gusano conocido como Wannacry ransomware, que afectó a más de 150 países y a casi 250.000 ordenadores[2], desconociéndose quién o quiénes fueron los creadores, autores de la propagación inicial y desde dónde se inició el ataque.

Las referidas formas de delincuencia, a modo de ciberataque, como el hacking o el phishing, han sido objeto de tratamiento en la Ley Orgánica 1/2015 de 30 de marzo, por la que se modificó el Código Penal, que tipificó entre otras estas conductas, propiciando como hemos señalado, nuevos tipos delictivos o adaptando los tipos

[1] AGUILERA LOPEZ (2003:102) “es un código malicioso incrustado en el código normal de un programa anfitrión. El virus se propaga de un ordenador a otro, pero para ello necesita la intervención humana. Puede afectar al funcionamiento del software y a las propiedades de la información y causar un impacto desde leve a muy grave sobre su objetivo… Las principales diferencias entre el gusano y el virus son que el primero no necesita la intervención humana para propagarse, pues lo hace de forma automática, y que no necesita alojarse en un código anfitrión. Se adueñan de los servicios encargados de la transmisión de datos para tomar su control”.

[2] https://elpais.com/tecnologia/2017/05/16/actualidad/1494927608_413489.html.“El ataque informático perpetrado el pasado viernes 12 de mayo puso en evidencia los sistemas de protección de multitud de empresas a lo largo del mundo. Muchas de ellas, que no habían instalado el correspondiente parche de seguridad enviado por Microsoft hace dos meses, han visto cómo muchos de sus datos se encuentran "secuestrados" tras el impacto del virus WannaCry, que se ha extendido a más de 150 países y ha infectado a casi 250.000 ordenadores, considerándose el más dañino de la era Internet.” Fecha de última consulta 07/06/18.

penales ya existentes. Dicho nuevo orden de ciberdelitos se soporta mediante las nuevas tecnologías ya sea como medio, como objeto o finalmente, respecto de lo que estuviera en relación con bien jurídico protegido.

El legislador decidió introducir, en dos modificaciones sucesivas en nuestro Código Penal, en los años 2010 y 2015, esta y otras definiciones relacionadas con los delitos informáticos y de las telecomunicaciones, aunque no hemos de obviar que los avances de las tecnologías nos adelantan social y culturalmente con mayor velocidad que la respuesta o respuestas que pudieran requerir desde el punto de vista legislativo y de protección judicial.

Con carácter previo a esta modificación de la norma, se dio cuenta de estos aspectos por parte del Consejo de la Unión Europea, como, por ejemplo, mediante la Decisión Marco 2005/222 del Consejo, de 24 de febrero de 2005, en relación con los daños informáticos, que con posterioridad fue modificada por la Directiva 2013/40 UE del Parlamento Europeo de 12 de agosto de 2013.

I.2. Objetivos

Los objetivos del presente trabajo, teniendo en cuentas los aspectos descritos en el apartado anterior, serán:

Describir las reformas de 2010 y 2015, mediante la LO 5/2010, de 22 de junio y LO 1/2015, de 30 de marzo, por las que se modifica el Código Penal, en el ámbito de las materias señaladas en el ámbito del presente trabajo, teniendo como punto de partida el Convenio Europeo de Europeo de Ciberdelincuencia de 2001 y las normas europeas posteriores.

Referir y delimitar las nuevas conductas delictivas según lo dispuesto en los art. 264 y 197, entre otros, del Código Penal, y sus tipos penales, sin perjuicio del análisis de cualquier otro delito tipificado que tenga relación con otros aspectos de las tecnologías de información y la comunicación, así como con la propiedad industrial y/o intelectual, analizando, entre otros aspectos, la conducta típica, los elementos materiales, el bien jurídico que protegen, los sujetos activos y pasivos, el resultado, concurso de delitos y concurso de penas, etc.: Delito de daños informáticos (art. 264 CP más los art. 264.bis, ter y quater, añadidos en la última reforma de 2015) en relación con delito de intrusión informática (art. 197 CP) y en su caso, en relación con el delito de estafa (art. 248 CP)

Analizar el ámbito espacial y temporal de la comisión de los posibles delitos, considerando el Principio de Territorialidad en el ámbito del Derecho Penal, delimitando aspectos fundamentales como el lugar donde se produce el delito y la consumación del resultado, dando la visión del derecho comparado.

Por ultimo, señalar las conclusiones sobre los retos que suponen para esta rama del Derecho de las Tecnologías de la Información y la Comunicación, y su tratamiento jurídico presente y futuro en relación con el Código Penal, indicando las insuficiencias prácticas que plantea esta regulación y también los retos necesitados de atención urgente por el legislador.

I.3. Metodología

El punto de partida de este trabajo, conforme a los objetivos señalados, será la definición de un problema jurídico que identificaremos y sobre el que trataremos de proponer una solución, convirtiéndose en el hilo conductor que ponga foco en el análisis y desarrollo del mismo.

Seleccionaremos, analizaremos y sintetizaremos información para poder formular una opinión y reflexión personal sobre el título planteado.

Compararemos aspectos jurisprudenciales y doctrinales desde la reforma e introducción de estos nuevos tipos penales, los distintos delitos contemplados en el Código Penal, atendiendo no sólo a la última reforma de estos, operada por la LO 1/2015, sino también a la más reciente jurisprudencia.

I.4. Agradecimientos

A mi mujer Natalia y a mis hijos, Carmen y Alejandro, por su comprensión y ánimo durante todo este tiempo de estudio y aprendizaje.

A mis compañeros de estudios, Amparo García y Jorge Espí, por su apoyo y aliento.

A mi profesor Sergio Cámara por haber despertado mi máximo interés en la asignatura de Derecho Penal y a la UNIR, que ha sido mi casa virtual durante estos años de estudio, así como a cada profesor que ha contribuido en mi formación.

A mi director, Francisco José Rodríguez, por su tiempo y dedicación.

Este trabajo que culmina una etapa ha sido gracias a ellos.

II. DEFINICIÓN Y ANTECEDENTES DE LAS CONDUCTAS DE HACKING Y PHISHING.

II.1. Definición de los ciberdelitos de hacking, phishing.

La Real Academia Española de la Lengua[3] define informática como conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. Podemos definir sistema de información, como equipo o conjunto de equipos unidos mediante una interconexión, que automatizan el uso y manejo de los datos contenidos en sus unidades de almacenamiento, mediante la ejecución de un programa o aplicación que los trata, recupera o transmite para su custodia, funcionamiento y transformación en conocimiento. Aunque antes de llevar a cabo el análisis concreto de los tipos penales mencionados, es necesario hacer mención a la novedad que ha supuesto en el Derecho penal, el camino que ha tenido que elegir el legislador en el momento de definir y reglar aquellos tipos penales relacionados con la evolución de las tecnologías y los sistemas de información, fundamentalmente por tratarse de materias novedosas que aparecen en nuestras vidas no hace más de cuarenta años

[3] http://dle.rae.es/?id=LY8zQy3. Fecha de última consulta 07/06/18

y que debido a su novedad y a la especial relevancia social, va a adquirir un especial protagonismo en el conjunto del Derecho.

Los países de nuestro entorno han definido a lo largo de estos años un marco legislativo que parte de la doctrina ha venido a denominar Derecho de la informática[4], que se podría definir como aquella rama del Derecho que tiene por objeto regular todos aquellos aspectos relacionado con el marco y medios en los que se desarrollan las estructuras informáticas. En este contexto actual, podemos definir ciberespacio[5] como un ecosistema de intercambios, conocimiento, datos, conexiones y enlaces, que crece exponencialmente como red en nuestras relaciones. Este universo está simultáneamente en todos los lugares y en ninguno de ellos, conformando infinitos lugares sin fronteras donde cualquier persona o entidad puede actuar, sin tener en cuenta un territorio o espacio físico concreto. Con esta concepción, el ciberespacio es un universo de infinitos lugares con infinitas características, por lo que, desde la óptica del Derecho, supone una gran dificultad, que analizaremos en los siguientes apartados del trabajo, teniendo en cuenta aspectos relevantes de lugar o tiempo.

Dentro de este marco se plantean necesariamente un compendio de problemas jurídicos – penales específicos de este nuevo tipo de delincuencia, atendiendo no sólo al perfil especial de los delincuentes, los hackers (del inglés, piratas informáticos) sino también a los problemas de persecución y anonimato que suponen.

Ahora podemos hablar de aspectos específicos tales como el intrusismo o interceptación de las comunicaciones, los daños y sabotajes, la protección de la privacidad, el abuso de sistemas, las estafas cometidas a través de ataques ransomware o también los delitos contra la propiedad intelectual relacionados con todos ellos.

El término hackear o piratería informática, puede definirse como la actividad ilegal que utiliza un equipo informático para acceder a información almacenada en otro equipo o sistema informático o para llevar acciones de difusión de virus informáticos. El diccionario de la RAE[6] define hacker o pirata informático como: “Persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta.”

Definimos el término “phishing” (del inglés, fishing[7], pesca) como la actividad dirigida a sustituir de forma fraudulenta la identidad de una persona o entidad con el objeto de adueñarse de forma indebida de datos confidenciales de acceso y contraseñas de los usuarios para, lograr deteriorar o desprestigiar su imagen o apropiarse de su patrimonio. La conducta típica consiste en que el estafador, (del inglés, phisher) consigue información de datos personales o empresariales mediante artimañas

[4] SUÑE LLINAS (2002:3) “El Derecho Informático […] es la disciplina que engloba a la Informática Jurídica y al propio Derecho de la Informática”.
[5] LESSIG (2001:6) “Existe la creencia de que el ciberespacio no puede ser regulado; que es, en esencia, inmune al control del Estado o de cualquier otro agente”
[6] http://dle.rae.es/?id=T8ktrp2. Fecha última consulta 07/06/18
[7] JARA (2012:300) “El término phishing, en informática, denota un uso de la ingeniería social para intentar adquirir información confidencial, por ejemplo, contraseñas, cuentas bancarias, datos de tarjetas, etcétera, de manera fraudulenta”.

fraudulentas, llevándose a cabo normalmente mediante un mensaje enviado por correo electrónico o por la suplantación de un acceso mediante una página web falsa o simulada, procediendo con posterioridad a la estafa con apropiación del patrimonio o sustitución de la identidad ajena.

II.2. El ransomware y el ciberataque del gusano Wannacry de 12 de mayo de 2017.

II.2.1. Definición de ransomware.

Los denominados ataques ransomware[8] (de "ransom", rescate en inglés, y "ware" por "software" o programa informático), se producen mediante un programa informático de código malicioso, que permite a los cibercriminales infectar equipos y sistemas informáticos, dotándoles de la capacidad de acceder a los mismos, bloqueando su acceso al usuario desde una dirección IP[9] remota (en inglés, Internet Protocol, dirección física vinculada al protocolo de internet) así como de la capacidad para encriptar datos y archivos ubicados en sus discos duros y servidores.

Este software, del que se tiene constancia por primera vez en el año 1989[10], es utilizado por sus creadores para obtener beneficios económicos, usualmente mediante el pago de un rescate del equipo a través de las denominadas criptomonedas o monedas virtuales, con la realización de un pago no trazable.

Según el Centro Criptológico Nacional (CCN-CERT), los ciberataques de tipo ransomware pueden tener diversas formas de acceso[11], entre las que podemos destacar: Phishing, causando la infección a través de un fichero adjunto de un correo electrónico o a través de un enlace a una página web simulada que incluye el código malicioso. Mediante accesos web a páginas cuyos servidores han sido atacados con carácter previo. O mediante métodos de averiguación de contraseña, como los denominados ataques de fuerza bruta, realizados a través de protocolos de control remoto, para obtener las contraseñas de acceso a servidores y a partir de las cuales puedan propagarse por el resto del sistema.

II.2.2. El ataque del gusano Wannacry

El ataque[12] de 12 de mayo de 2017, fue un ataque informático mediante el denominado gusano Wannacry, de tipo ransomware con capacidad para infectar otras máquinas, llevado a cabo infectando ordenadores de más de 150 países que utilizaban el sistema operativo Windows (Microsoft) y afectando entre otros a España, dónde, grandes empresas como Telefónica, Gas Natural o Repsol, fueron víctimas del virus, quedando gran parte de los datos de sus equipos encriptados, y sobre los que el autor o autores solicitaban el pago de un rescate económico para

---

[8] https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/. Fecha de última consulta 07/06/18

[9] ESPAÑA BOQUERA (2003:180): "Las direcciones IP, también conocidas como direcciones de internet, identifican de forma única y global a cada sistema intermedio y a cada sistema final ."

[10] CASAS HERRER (2017:160): "Por su forma de operar, se clasifica entre los troyanos, es decir, aquellos que toman el control de un ordenador. Dentro de estos, se denomina, ransomware, que se puede traducir como "programa que pide un rescate". ... En 1989 se tuvo conocimiento del primero de estos troyanos, conocido como AIDS... Estaba programado por el estadounidense Joseph Popp"

[11] CCN-CERT (2017): "Guía Buenas Practicas BP-04/16: Ransomware"

[12] https://blog.avast.com/es/ransomware-telefonica-hospitales. Fecha de última consulta 07/06/18

desbloquear el acceso a los mismos. El CCN-CERT[13] alertó de un ataque masivo de ransomware que aprovechaba una vulnerabilidad en equipos o sistemas que utilizaban el sistema operativo Microsoft Windows, obstruyendo y bloqueando el acceso a los datos contenidos tanto en las unidades de almacenamiento de los mismos, como en unidades locales y los contenidos en las redes a las que pudieran estar conectadas, comprometiendo a su vez la seguridad de todos los equipos y sistemas de las redes de la organización, siempre que no estuvieran debidamente actualizadas y protegidas.

El gusano infectaba cada equipo o sistema informático cifrando todos o parte de sus archivos, utilizando la vulnerabilidad denominada EthernalBlue, que permitía la ejecución remota de comandos maliciosos y distribuyéndose al resto de equipos con sistema operativo Windows que hubiera en esa misma red. Es decir, el autor o autores fue o fueron capaces de entrar en los ordenadores y sistemas mediante el uso de lo que se denomina un código malicioso (del inglés, exploit) que permite acceder al equipo sin que el legitimo propietario pueda hacer nada, siendo sólo necesario que esté encendido y conectado a internet; y lo que le da mayor relevancia al ataque es que en cuestión de horas fueron afectados cientos de miles de ordenadores de todo el planeta. Cuando el Wannacry entraba en un ordenador, fingía inicialmente ser únicamente ramsonware, encriptando todos los archivos del equipo, solicitando un rescate para descifrar todos los ficheros y archivos bloqueados. Sin embargo, su objetivo también estuvo dirigido a paralizar, inutilizar o incluso destruir el propio equipo o sistema informático.

Servicios públicos y hospitales de todo el mundo, como el Servicio Nacional de Salud de Gran Bretaña (NHS), la Deutsche Bahn AG, principal empresa ferroviaria de Alemania, compañías aéreas como la chilena LATAM también resultaron atacados, afectando al normal funcionamiento de dichos servicios para pacientes o usuarios, o a la posibilidad de enfrentarse a la amenaza de una pérdida definitiva de los datos en el supuesto de no pagar el desbloqueo de los equipos, previa entrega de 300 dólares, en bitcoins[14].

La cuestión reside además en que no hay nada que impida a los hackers llevar a cabo esa misma conducta delictiva, por ejemplo, en cualquier sistema informático de la red de energía de un país, desde una ignota dirección IP, ubicada en un ignoto servidor, entrando en uno o dos puntos clave de la red, crear un efecto dominó y afectar a toda la red eléctrica de ese país. Podemos imaginar lo que ocurriría si toda la red eléctrica deja de funcionar: todo deja de funcionar, el suministro de agua, los servicios básicos, sanitarios… todo, porque todo está conectado con todo.

Bajo la perspectiva del análisis del tipo que llevaremos a cabo más adelante, es reseñable que, una vez infectado el equipo o sistema, el autor evita que se pueda utilizar, bloquea su funcionamiento o impide el acceso a sus datos, salvo que se pague una cantidad en moneda virtual mediante plataformas de pago poco

[13] CCN – CERT: Comunicado publicado el 12 de mayo de 2017 a través de su página web https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html. Fecha de última consulta 07/06/18.

[14] https://computerhoy.com/noticias/software/corea-del-norte-fue-responsable-wannacry-segun-nsa-63680. “Una vez dentro, infectaba el ordenador y automáticamente bloqueaba todos los archivos. Para liberarlo exigía un rescate de 300 dólares en monedas bitcoin para restaurar el sistema.” Fecha de última consulta 07/06/18.

rastreables. Los importes del pago de los rescates se ubicaron en las denominadas carteras (en inglés, wallets), estimándose un importe total en torno a 70.000 dólares, almacenados de forma anónima, y que no habían sido retirados por parte de los supuestos cibercriminales, probablemente para evitar ser rastreados, tratando por tanto de evitar su identificación e impidiendo iniciar su persecución penal por dichas supuestas conductas delictivas.

III. EL DELITO DE DAÑOS INFORMÁTICOS. EVOLUCIÓN Y MARCO NORMATIVO

III.1. Convenio Europeo sobre Ciberdelincuencia de 2001

La Convención Europea del Consejo de Europa, en materia de Ciberdelincuencia se celebró en Budapest, firmándose en fecha 23 de noviembre de 2001 el Convenio sobre Ciberdelincuencia[15], que posteriormente fue ratificado por España mediante Instrumento de Ratificación de fecha 20 de mayo de 2010, publicado en el Boletín Oficial del Estado de 17 de septiembre de ese mismo año. Entre los aspectos relevantes recogidos en su preámbulo[16], se señala la necesaria obligación por parte de los Estados miembros, de aprobar e implantar una política común eficaz en materia penal mediante la adaptación de las legislaciones de cada estado, la cooperación y la capacidad de respuesta ante los aspectos derivados de la digitalización y la globalización de las redes informáticas. En su articulado se introduce la terminología adecuada para definir y distinguir entre otros, sistema informático, datos informáticos, o, proveedor de servicios informáticos, señalando las medidas que deberán adoptarse en cada estado dentro de su ordenamiento penal en los denominados delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos[17], refiriéndose expresamente, entre otros, a los accesos ilícitos deliberados e ilegítimos a la totalidad o parte de un sistema informático, infringiendo medidas de seguridad, la comisión deliberada e ilegítima de actos que ataquen la integridad de los datos o del sistema y abusos, falsificaciones o fraudes, con la intención dolosa de obtener de un beneficio para sí mismo o una tercera persona.

III.2. Normativa europea: Decisión Marco 2005/222 y Directiva UE 2013/40.

La Unión Europea, mediante la aprobación de la Decisión Marco 2005/222/JAI[18] del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, dio un paso adelante en materia de ciberseguridad, estableciendo una finalidad principal dual: en primer lugar, la necesidad de establecer una armonización de normas comunes de la materia para la totalidad de Estados miembros, a través de la definición de ilícitos penales así como de las sanciones aplicables y, en segundo lugar, reforzar la cooperación entre todos ellos y sus organismos judiciales y policiales.

---

[15] Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia. Fecha de última consulta 07/06/18.

[16] Preámbulo, Convenio sobre la Ciberdelincuencia: “Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos …”.

[17] Art. 1 y ss. Convenio sobre la Ciberdelincuencia.

[18] https://www.boe.es/doue/2005/069/L00067-00071.pdf. “El objeto de la presente Decisión marco es reforzar la cooperación entre las autoridades judiciales y otras autoridades competentes, …”; fecha de última consulta 07/06/18.

La Directiva 2013/40/UE[19], de 12 de agosto, relativa a los ataques contra los sistemas de información, otorga respuestas a las nuevas conductas delictivas relativas a injerencias en sistemas informáticos ajenos, así como a nuevas formas de incurrir en daños informáticos, que aparecen diferenciados, como no podía ser de otra manera, en la citada norma. Desarrolla aspectos relevantes en la definición de tipos penales relativos a los ciberataques, que pueden ir, por ejemplo, desde los denominados ataques de denegación de servicio, diseñados y realizados contra el funcionamiento de un servidor, la interceptación de equipos y datos, como puede ser el caso que nos ocupa, hasta los ataques de botnets, tipificándose todos ellos.

Ambas normas, la Directiva de 2013 al igual que la Decisión Marco de 2005, tienen origen en el Convenio de Ciberdelincuencia de 2001.

III.3. Concepto y definición de daños informáticos.

Antes de adentrarnos en la definición del concepto de daños informáticos, hemos de tratar la figura del delito de daños, que está referido a la destrucción o deterioro funcional de un bien material de propiedad ajena, de forma que dicho bien resulte averiado, deteriorado o destruido por el resultado de una acción llevada a cabo.

Constituyen las denominadas infracciones penales patrimoniales en las que el legislador, en la redacción de la norma penal, no consideró el enriquecimiento del autor material entendiendo la acción típica de los sujetos activos no conlleva la incorporación a su patrimonio o al de un tercero de la cosa dañada, no existiendo por tanto ánimo de lucro. Los daños requieren el menoscabo, deterioro o destrucción del bien jurídico protegido ajeno, la propiedad, ya sea esta de titularidad pública o privada.

En este conjunto de delitos nos vamos a encontrar con conductas o acciones típicas dolosas, esto es, que requieren que el autor o autores tengan la conciencia y voluntad de realizar la acción dañosa, o, dicho de otro modo, que esta se lleve a cabo a sabiendas, con intención maliciosa. La jurisprudencia del Tribunal Supremo señala esta cuestión referida al "animus nocendi"[20], esto es, el ánimo de dañar[21], no exigiendo que la acción se lleve a cabo con el ánimo de lucrarse.

---

[19] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al33193. “La presente Directiva introduce nuevas normas que armonizan la criminalización y las penas para varios delitos contra los sistemas de información. Estas normas incluyen la ilegalización de la utilización de los denominados «botnets»: programas nocivos diseñados para tomar el control remoto de redes de ordenadores.” Fecha de última consulta 07/06/18.

[20] STS, Sala de lo Penal, de 28 de Octubre 1991 (LA LEY 550/1992): “Que, en todo caso, el delito de daños exige, según reiterada jurisprudencia, dos requisitos: 1º) el resultado de daños; y 2.º) la intención de perjudicar con tal daño a un tercero «animus nocendi»”.

[21] Fernández Aparicio: (Diario La Ley, Sección Doctrina, 1998, Ref. D-270, tomo 5, Editorial LA LEY-21326/2001: “Según reiterada jurisprudencia (sentencias de 4 de noviembre y de 2 de diciembre de 1982, de 29 de marzo de 1985 y de 17 de septiembre de 1986) dicha figura punitiva ha de entenderse cometida cuando a medio de la actuación voluntaria de una persona se origina la inutilización, destrucción o deterioro de cosas de ajena pertenencia protegidas por el derecho y valorables en su concreto detrimento exigiéndose el dolo específico constituido por el animus damnandi o nocendi que en su intención final se dirija conscientemente a destrozar o menoscabar los bienes o intereses de tercera persona.”

En cualquier caso, el Código Penal no nos refiere una definición como tal del concepto de daños, sino que lo hace de forma indirecta al referirse a los bienes jurídicos que puedan resultar afectados. La definición legal del concepto de daños informáticos en nuestro ordenamiento responde, como ya nos hemos referido, a la regulación señalada por las instituciones del Derecho europeo.

Cuando nos referimos al concepto de delitos informáticos hemos de tener en cuenta que definimos una conducta delictiva llevada a cabo por medio de elementos tecnológicos, esto es, se trata de acciones realizadas mediante un programa o código informático para su comisión, que además puede ser llevado a cabo, no sólo mediante un equipo informático, sino también, mediante otros artilugios tecnológicos como pueden ser un teléfono móvil con conexión a internet, una tableta, etc.

El artículo 264.2 del Código Penal se introdujo en nuestro ordenamiento jurídico con la redacción dada por la L.O. 10/95, de 23 de noviembre, que establecía que la misma pena se impondrá a quién por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos.

El tipo se definió como un tipo agravado del delito de daños, por el que se abordaba el problema surgido por el desarrollo de las tecnologías y fundamentalmente, dotando de una respuesta a los desarrollos y las difusiones por parte de los hackers, de virus informáticos, o a la alteración de equipos y sistemas, cuestión a la que nos hemos referido en apartados anteriores. Esto es debido a que la redacción inicial del art. 264 CP estaba encaminada a dar respuesta al tipo básico del delito de daños, en el que se definían con carácter general, fundamentalmente, aquellos que se producen sobre objetos materiales. Por esto anterior, el legislador introdujo el tipo referido a los daños informáticos, dotándole de autonomía y naturaleza propia, frente al tipo básico señalado en el art. 263 CP, incluyendo las posibles conductas descritas en los apartados anteriores, pensando con acierto, en la intangibilidad de algo tan intangible como pueda ser un código o programa informático.

Debemos valorar la gravedad de los daños informáticos mediante la evaluación de la pérdida de funcionalidad del bien jurídico objeto del delito, no confundiendo el elemento del tipo, daño directo con el posible perjuicio ocasionado. Los gastos derivados de la restauración de los sistemas afectados, el antivirus de protección, un posible lucro cesante, etc., debemos considerarlos como elementos que no integran el concepto del daño, sino que podrán ser objeto de reclamación por responsabilidad civil.

Cabe señalar por su relevancia, que nos encontramos ante una diferencia fundamental respecto al tratamiento que hace el legislador respecto al valor patrimonial dañado, señalando que este suponga una valor superior a 400 euros, mientras que cuando se refiere al resultado del tipo de daños informáticos no hace referencia a ningún valor económico sino que solamente se refiere a que el resultado y su valor económico debe ser grave, sin determinar cuál sería la cuantía delimitadora de dicha gravedad.

III.4. Las reformas del Código Penal de 2010 y 2015

La Decisión Marco 2005/222/JAI fue transpuesta a nuestro ordenamiento interno, a través de la 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, introduciendo la

tipificación específica de los delitos de daños informáticos en su artículo 264[22], dentro del conjunto global de la definición del delito de daños. Por otra parte, se procedió a la modificación del art. 197 y concretamente a la tipificación de la intromisión ilegal a los sistemas informáticos, , así como otro aspecto novedoso, relativo a la previsión, en el párrafo segundo, de las penas correspondientes con la responsabilidad penal de las personas jurídicas, no sólo de las personas físicas en aquellas acciones en que resultaran responsables de las conductas ilícitas señaladas cuando concurriesen las circunstancias previstas en el art. 31bis del mismo texto legal.

Por último, el legislador, en relación con lo establecido en la Decisión Marco, introducía aspectos relevantes como la agravación específica cuando nos encontremos ante supuestos que causaren daños cometidos en el marco de una organización criminal o bien, resultasen de especial gravedad o se produjeran afectando a los intereses generales.

Esta modificación, dio solución a las obligaciones contraídas por España en el marco de la cooperación y la armonización jurídica europea, que exigía la adaptación de nuestra norma penal[23].

La reforma operada entró en vigor el 23 de diciembre de 2010, y vino a ampliar, como hemos señalado, las circunstancias que daban cualificación distinta del tipo básico de daños, otorgándole la necesaria autonomía para ser aplicada como tal por el juzgador, distinguiendo en dos grupos las conductas punibles, apartados primero y segundo, y las penas aplicables en relación con la relevancia y gravedad de cada uno de ellos. Esta autonomía la distinguía, el caso de este tipo de daños informático, al considerar que no resultaba tomar en consideración el criterio de los 400 euros[24] para poder considerarlos como delito tal y como lleva a cabo el art. 263 CP.

La redacción del art. 264.2 del Código Penal, pareciendo estar dirigida de modo particular a delimitar las conductas llevadas a cabo por los crackers, imponía la pena de prisión de seis meses a tres años a quien “por cualquier medio destruya, altere, inutilice o de cualquier modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos”.

En cualquier caso, el legislador entendió que la conducta típica se había de llevar a cabo sin autorización del sujeto pasivo y de modo grave, así como que el resultado habría de ser grave igualmente, si bien, otra cuestión relevante, a la que parece dejarse libertad de apreciación por el juzgador, es la de distinguir entre aquellas conductas que pudieran ser relevantes y aquellas otras que no lo serían, siendo la gravedad un elemento esencial para que exista conducta criminal.

---

[22] Art. 264 CP: “1. 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. 2. 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.”

[23] BERDUGO GÓMEZ DE LA TORRE (2016:98).

[24] SAP de Sevilla, Sección 7ª, de 30 de diciembre de 2011, Rec. 6474/2010.

Posteriormente, la modificación del texto penal operada por la Ley Orgánica 1/2015, de 30 de junio, ha venido a introducir la tipificación de las conductas graves llevadas a cabo mediante ataques que obstaculicen o interrumpan el normal funcionamiento de los sistemas de información ajenos. Esta reforma modificó en modo notorio la regulación disponible en la materia hasta la fecha, creando un nuevo precepto teniendo en cuenta la transposición a nuestro ordenamiento jurídico de la Directiva 2013/40/UE. Es relevante y por ello lo resaltamos, el hecho de que el legislador europeo vino a señalar los comportamientos delictivos de manera no cerrada, para así poder incluir toda clase de ilícitos.

La sustitución en el marco normativo europeo de la Decisión Marco por la Directiva de 2013 determinó por tanto la obligación de adecuar nuestra regulación penal a adaptaciones con las que se pretendió dar respuesta a los problemas y situaciones generadas como consecuencia de posibles ataques coordinados de gran tamaño a los sistemas de información.

La reforma operada en nuestro ordenamiento tuvo como objetivo trasladar el contenido de la norma europea a la nueva redacción dada a los artículos 264, 264.bis[25] y 264.quater, todos ellos dentro del capítulo IX del Título XIII CP, de los daños, transfiriéndose prácticamente el contenido de la Directiva referida a las actuaciones o interferencia en los sistemas, art. 264.bis apartado 1, y los relativos a las actuaciones o interferencias en los datos, en este caso, mediante la modificación del art. 264.1, e incorporando, mediante el art. 264.ter, los aspectos relevantes a la tenencia de instrumentos, programas o contraseñas y códigos de acceso o similares que permitan acceder a la totalidad o a una parte de un sistema informático. El art. 264.quater prevé las consecuencias penales para aquellas conductas cometidas por una persona jurídica.

Respecto a las penas, se castigan ahora las conductas tipificadas, desde los seis meses a tres años de prisión, imponiéndose en su mitad superior e incluso a la superior en grado cuando se realicen mediando las circunstancias previstas en el art. 264.2, afectaran de forma relevante a una empresa, negocio o Administración pública, o se usaran ilícitamente datos de terceras personas.

El legislador español introdujo un nuevo artículo, el 197.bis, dentro del capítulo I del título X referido a la vulneración de medidas de seguridad y acceso a sistemas de información o se mantenga dentro de él sin estar debidamente autorizado, castigándolo con una pena de prisión de seis meses a dos años.

Por último, hemos de señalar que la LO 1/2015 añadió un nuevo artículo, en este caso, el art. 127.bis.1.c), que introduce la referencia al término de delitos informáticos contra la intimidad y de daños definidos en el artículo 197 apartados dos y tres, y artículo 264, respectivamente.

[25] Art. 264.bis: “Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo anterior; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.”

IV. ANÁLISIS DEL TIPO PENAL DEL DELITO DE DAÑOS INFORMÁTICOS EN NUESTRO SISTEMA PENAL.

En el análisis penal del ataque del gusano Wannacry, nos encontramos con una serie de dificultades dentro del concepto técnico-jurídico del delito, de la antijuricidad, las causas de justificación y la culpabilidad, por lo que hemos de profundizar en los conceptos de acción y omisión como elementos iniciales de la definición de delito, la tipicidad, la relación de causalidad en el tipo o tipos incardinados en los artículos 264 y ss., 197.bis y en su caso, el 248 y ss. CP, las causas de exclusión de las posibles acciones y omisiones, la relevante problemática respecto de la determinación del sujeto o sujetos activos en las diferentes conductas delictivas, el atolladero del tiempo y lugar de comisión de los delitos, sobre todo esto último en relación con el denominado Principio de Territorialidad, así como a los criterios de imputación objetiva y los elementos intencionales, intelectuales o volitivos, pudiendo estar incluso ante meras acciones imprudentes de los posibles sujetos pasivos en relación con los bienes jurídicos afectados, que pasamos a desarrollar a continuación.

IV.1. Análisis del bien jurídico protegido.

El delito de daños se encuentra regulado en el Capítulo IX del Título XIII del Código Penal. En el mismo, el legislador ha incluido y delimitado una pluralidad de figuras delictivas en el ámbito del patrimonio, en el ámbito de la informática y las telecomunicaciones, pero también resulta evidente que estamos ante un bien jurídico novedoso, al igual que las conductas delictivas analizadas, que ha de tener necesariamente relación con la seguridad de los sistemas informáticos.

Si nos atenemos a lo señalado en el art. 264.1 CP, el bien jurídico protegido ha de ser por una parte el patrimonio, y por otra, el orden socioeconómico, en cuanto que se refiere a la afectación de infraestructuras críticas para el funcionamiento del Estado o a las funciones vitales de la sociedad como la salud, la seguridad o la protección y el bienestar económico y social de la población.

Respecto a la valoración de los daños hemos de determinar, asimismo, cuál es el perjuicio causado tanto a nivel particular, respecto del patrimonio individual, como a nivel global, que impidió de manera grave, por ejemplo, al operador de telecomunicaciones, dar un servicio a sus clientes, así como los posibles perjuicios patrimoniales causados a la misma por las posibles demandas a las que se podría enfrentar por afectación y caída de sus sistemas y redes y el no funcionamiento de los servicios esenciales de la comunidad, como por ejemplo, hospitales, policía, bomberos, etc., y así como a los particulares usuarios de los mismos. Recordemos que aquí la conducta expuesta no busca inicialmente obtener un lucro sino dañar el software o los datos de los equipos del sistema.

En relación con los daños que afectan a una infraestructura crítica en relación con la protección que establece el art. 264.2.4ª, podría el ataque del gusano Wannacry sufrido por Telefónica entenderse como perjuicio a un servicio público, aunque no sea una entidad directamente pública y estar privatizada, dado que puede entenderse que se hubieran ocasionado daños de especial gravedad, perjuicio grave a los servicios públicos, entendidos como bienes jurídicos protegidos.

E incluso, de forma indirecta nos estamos refiriendo al patrimonio como bien jurídico protegido no por la acción directa de las conductas llevadas a cabo sobre los equipos de los sujetos pasivos sino por las consecuencias que se derivan de aquellas.

Por otra parte, en el supuesto podemos encontrar un aspecto determinante en relación con la intromisión del sujeto activo en la intimidad, aspecto referido al art. 197 CP y la seguridad del sujeto pasivo, que debemos considerar como bien jurídico protegido[26], si nos referimos a los aspectos descritos en los art. 264, bis, ter y quáter.

IV.2. El tipo objetivo.

Tras habernos referido a la evolución temporal de la regulación de nuestro ordenamiento penal en la materia estudiada, debemos ahora abordar los aspectos relativos a los tipos objetivos de las diferentes conductas típicas descritas en los artículos 264, bis, ter y quáter, tras la reforma operada por la LO 1/2015. Respecto al art. 264.quáter, como hemos señalado anteriormente, hemos de observar que hasta la reforma operada por la LO 5/2010 no podría imputarse a personas jurídicas, sino que sólo cabía determinar la responsabilidad penal de las personas físicas.

En el análisis del tipo objetivo, como representación del aspecto físico o externo de la conducta típica, hemos de hacer referencia a las acciones típicas y a los resultados producidos por las conductas señaladas para con ello analizar si en los posibles delitos cometidos se requiere un delito de resultado o si estamos ante delitos de mera actividad. Dentro de este análisis debemos distinguir los elementos que describen el tipo, como la conducta, la relación de causalidad y la imputación objetiva, encontrándonos, a nuestro parecer, con un problema respecto a este último elemento, como es la imputación de un resultado a un desconocido sujeto activo, cuestión sobre la que profundizaremos a continuación.

IV.2.1. Sujetos activos.

En el delito, como sujetos de la acción, podemos distinguir entre sujeto activo, quién realiza la acción o conducta delictiva, y el sujeto pasivo, como titular del bien jurídico lesionado por el sujeto activo.

Respecto a esta figura, en general, debemos identificar personas físicas o jurídicas que pudieran ser objeto de análisis, las cualidades de cualquiera de dichos sujetos que puedan tener relevancia típica jurídica que distinguiese entre delitos comunes y especiales, y determinar si existiera relación con los sujetos pasivos, en su caso.

Nos encontramos ante un delito común, esto es, que puede llevarse a cabo por cualquier persona física o persona jurídica, no requiriéndose reunir ninguna cualificación especial y siempre que ninguna de ellas fuese el propietario de los bienes jurídicos atacados.

[26] GALÁN MUÑOZ (2006:30): “Este planteamiento [ubicar los tipos referidos a la informática en las categorías clásicas] resulta erróneo, por cuanto en realidad estos nuevos tipos delictivos vendrían a proteger unos bienes jurídicos diferentes y, sobre todo, cualitativamente más amplios”.

En nuestro particular análisis, en el delito de daños informáticos, el sujeto o sujetos activos serían, aquél o aquellos que crearon el Wannacry, programa o código malicioso, por una parte, o siendo los mismos o distintos, quién o quienes lanzaron el ataque y la conducta delictiva de propagación de este. También resultarían ser sujetos activos, aquellos quiénes de manera no autorizada se hubieran introducido en los equipos o sistemas informáticos, o quiénes de forma remota hubiesen bloqueado los mismos o los datos contenidos en ellos. Recordamos aquí de nuevo, que tras la reforma operada por la LO 1/2015, pueden ser sujetos activos tanto las personas físicas como jurídicas, conforme a lo señalado en el art. 31.bis CP.

Una cuestión interesante, a nuestro modo de ver, que podemos introducir, pero que sería objeto de un análisis distinto en otro trabajo al que estamos realizando, es la relativa a la posibilidad de que una cosa inanimada resultara ser el sujeto autor del delito del ataque. Si bien parece haber sido cometido por personas físicas o jurídicas, con la evolución tecnológica, cabría pensar, o probablemente no estemos lejos de entender, quizás ya lo estemos, que una máquina o sistema podría ser el creador del comando malicioso autoejecutable que pusiera en marcha la propagación del gusano. Estaríamos por tanto ante una conducta delictiva que puede haber sido iniciada por una cosa inanimada.

IV.2.2. Sujetos pasivos.

Los sujetos pasivos serían los titulares de los bienes jurídicos afectados. Puede ser una persona física o jurídica o el propio Estado o la Unión Europea.

Como titular del bien jurídico lesionado (patrimonio), que puede ser menoscabado o destruido, y de aquellos bienes jurídicos puestos en peligro (seguridad, intimidad o la protección del orden socioeconómico) que sólo requerirían la puesta en peligro de dichos bienes cuya protección garantiza el derecho, hemos de diferenciar entre el propio sujeto pasivo, como pudiera ser cualquiera de las personas o entidades cuyos equipos o sistemas resultaron afectados, como los posibles sujetos perjudicados por la afectación del funcionamiento de los servicios públicos esenciales a los que ya nos hemos referido al relatar el ataque, distinguiendo a su vez entre sujetos pasivos sobre los que recaen las distintas acciones, los sujetos pasivos titulares de los bienes jurídicos señalados y los perjudicados no titulares de los bienes jurídicos pero que de forma indirecta sufran las consecuencias lesivas derivadas de la comisión de los posibles delitos.

Aunque en ocasiones puedan coincidir, en este caso, hemos de diferenciar entre los sujetos pasivos, propietarios y/o titulares de los datos informáticos y de los equipos y/o sistemas, y el objeto material de las acciones realizadas, en este caso, las propias cosas o elementos afectados, cuestión que también resulta dificultosa, al encontrarnos tanto con aspectos tangibles como con aspectos intangibles.

La propia evolución de la tecnología nos lleva a preguntarnos qué ocurre con aquellos datos que no están físicamente ubicados en el equipo informático propiedad del sujeto pasivo, sino que por el contrario se encuentran alojados en lo que se ha venido a denominar almacenamiento en la “nube informática”[27] (del inglés,

[27] TORRES VIÑALS (2011:84): “El *Cloud Computing* es un modelo que permite el acceso bajo demanda a través de la red a un conjunto compartido de recursos de computación configurables…”

cloud computing). Hemos de referirnos a este aspecto porque pueden ocurrir dos situaciones distintas que nos revelan otra dificultad: la primera sería aquella en la que el propio sujeto pasivo, titular o propietario de los datos, se hubiera visto afectado por el ataque en su propio equipo o sistema; y la segunda, en la que el titular de los datos tuviera alojados los mismos en un servidor propiedad de un tercero, siendo este tercero no propietario de los datos o programas informáticos el sujeto pasivo atacado, y convirtiendo al titular de los datos en sujeto perjudicado que sufre las consecuencias de la acción.

IV.2.3. Conducta típica.

La acción[28] es una conducta humana[29], activa u omisiva, con transcendencia exterior que puede consistir en llevar a cabo voluntariamente lo que está prohibido (acción en sentido estricto, conducta activa o delito comisivo), o en no efectuar lo que se está obligado a hacer (conducta omisiva o delito omisivo). No existiría acción en aquellos supuestos en los que no cabría la posibilidad de atribuir la responsabilidad al autor o autores por haber actuado por acción de una fuerza irresistible, por movimientos reflejos o en estados de inconsciencia.

La tipicidad[30] es la descripción del delito que establece el Ordenamiento penal, por lo que es necesario que para que una acción u omisión pueda ser penalmente relevante ha de ser descrita por la ley, esto es, cuando una conducta se adecua a la descripción de la norma penal, podemos afirmar que la acción u omisión podría constituir un delito. En sentido contrario, no nos encontraríamos ante un delito cuando no se produce una adecuación a la definición dada por la norma penal o cuando los hechos no se pueden vincular a una conducta típica; aunque señalar o deducir la posibilidad de una conducta, no significa necesariamente que estemos ante una situación de ilícito penal en la que vaya a atribuirse la responsabilidad al sujeto activo, ya que como veremos en los apartados siguientes, además, se han de dar tanto el resto de aspectos de la tipicidad, así como de la antijuridicidad y la culpabilidad.

Con la definición dada en el art. 264.bis, la conducta típica estaría, al menos, en un sentido restrictivo, dirigida a la consecución de un resultado, como es en el caso que nos ocupa, la obstaculización o la interrupción del funcionamiento de un equipo o sistema informático ajeno, de modo grave y mediante las acciones referidas en el propio artículo, si bien como analizaremos posteriormente podemos estar ante conductas recogidas tanto en el art. 264.1 en relación con el 197.bis y como en el art. 264.ter.

En el supuesto del posible delito de mera actividad como el que puede asociarse a la conducta típica de la creación de un programa, virus o código malicioso, bastaría

[28] CEREZO MIR (1999:19): ”El primer elemento del delito en el Código penal español es una acción o una omisión… La acción o la omisión para que constituyan delito habrán de estar comprendidas en uno de los tipos de lo injusto del Código penal o de las leyes penales especiales”.
[29] MARTINEZ ESCAMILLA (2012:87): “El comportamiento (o conducta) en sentido jurídico penal es el primero de los requisitos exigibles respecto a cualquier hecho que se quiera (des)valorar desde el punto de vista penal. Este elemento común a todo delito puede consistir en una actuación positiva (acción) o en una omisión. Como tal requisito se encuentra recogido en el art. 10 CP.
[30] CEREZO MIR (1999:19):” La tipicidad, en el sentido de correspondencia a un tipo de lo injusto, es el segundo elemento del concepto de delito.”

comprobar que se ha realizado la conducta descrita en el tipo para que se haya cumplido la parte objetiva de aquél.

Como acción típica es preciso para el supuesto que tratamos, determinar que se hubiesen borrado, dañado, deteriorado, alterado, suprimido o hacer inaccesibles datos informáticos. En la descripción de los hechos del ataque, se produjo una acción de creación de un programa malicioso que se aprovechaba de una vulnerabilidad del sistema operativo, otra acción de acceso no autorizado a los equipos y sistemas de información de los sujetos pasivos, por las que se impedía, en primer lugar, el acceso a los datos informáticos contenidos en los equipos o sistemas, mientras que, en segundo lugar, se producía un borrado de los mismos, si no se accedía al pago del rescate de los mismos previo pago de la cuantía señalada por el atacante.

En una segunda consideración, podemos señalar que mediante el gusano Wannacry se producía la acción de dañar, inutilizar o eliminar el acceso al sistema informático.

Debemos distinguir pues, entre la actividad típica de un hacker, que hubiese accedido a los sistemas informáticos con la intención de obtención de información que posteriormente no hubiese destruido, siendo una conducta más propia del art.197 CP y la actividad de los denominados crackers, como aquellos quienes dolosamente habrían cometido los daños en los sistemas informáticos mediante el acceso y la infección de estos y que, de manera intencional, habrían violado la seguridad de cualquiera de los equipos y sistemas informáticos afectados para mediante la conducta referida, bloquear datos o programas informáticos o hacerlos inaccesibles, eliminar o borrar ficheros contenidos en ellos, así como introducir la secuencia del gusano que permitía su reenvío a otros equipos, estando en este caso ante acciones típicas del art. 264 y ss. CP. Por último, se debe determinar una conducta intermedia entre ambas, aquella que consistiría en alterar los datos, sin que el propietario del bien jurídico lo detecte o sin que ello menoscabe el funcionamiento del programa o sistema, por lo que podríamos encontrarnos con la dificultad de establecer si se produce o no una situación delictiva contenida en el art. 264.1 CP.

Podríamos, a nuestro entender, tratar de establecer una relación con la extracción del tipo básico de estafa del art. 248.1 CP, puesto que los autores inducían además al engaño a los sujetos pasivos, con ánimo de lucro (elemento subjetivo), llevando a cabo actos continuados de disposición de los datos de contenidos en los equipos y sistemas (elementos objetivos) mediante la utilización de la treta. La dificultad en este aspecto podría residir en que la posible estafa podría estar cubierta por el consentimiento del sujeto pasivo, que asumiera que la representación del error del tipo que se le efectúa pudiera ser incierta, dado que proveedores de seguridad informática y autoridades advertían de no acceder al pago del rescate exigido para liberar dichos equipos y sistemas informáticos de la acción de ataque.

Nos encontraríamos además ante un posible delito continuado, dada las conductas o modo de llevarse a cabo cada una de las acciones de infección, no constituyendo distintos delitos, sino que podría considerarse como un único delito de estafa hacia una generalidad de sujetos pasivos afectados y perjudicados, con notoria gravedad, pudiendo castigarse con uno o dos grados más en relación con lo señalado en el art. 74.2 CP.

A la descripción legal de cada una de las conductas penalmente prohibidas a las que se hace referencia en nuestro ordenamiento jurídico penal, la Teoría del delito, en relación con el elemento de tipicidad nos viene a decir que un hecho es penalmente típico cuando se halla previsto por la ley como tal tipo de delito[31], como podría dar lugar en este caso, ante los posibles delitos de daños informáticos, intrusión informática o estafa. Una de las conductas típicas del ataque, como ya nos hemos referido, consistió en lograr un resultado, como fue la obstaculización o interrupción del funcionamiento de sistemas informáticos ajenos, de manera grave y a través de alguna de las acciones indicadas, bien en el art. 264.1, haciendo inaccesibles datos informáticos o programas informáticos siendo grave el resultado producido, referido además, por haber afectado a infraestructuras críticas o esenciales para el mantenimiento de funciones vitales de la sociedad, como la salud, la seguridad, la protección, o bien, como señala el art. 264.bis, al haberse obstaculizado o interrumpido el funcionamiento de numerosos sistemas informáticos ajenos introduciendo o transmitiendo datos, y mediante otra conducta típica, como es la de intrusión informática, señalada en el art. 197.bis apdo. primero CP.

Resaltamos de nuevo aquí que, dada la redacción del tipo penal, para que el daño o daños se consideren incluidos en la conducta típica, estos se deben producir de manera grave produciendo además un resultado grave.

Entre los problemas iniciales reside la cuestión de averiguar y determinar quién creó e introdujo ese virus de tipo gusano en el primer equipo infectado, o si se utilizó o facilitó un programa o código informático malicioso concebido o adaptado fundamentalmente para las actividades que señala el art. 264.ter.

Ello implica la dificultad de poder castigarlo, debiendo recordar que estamos ante un delito doloso[32]. Por tanto, si se hubiese realizado imprudentemente, por ejemplo, introduciendo un pendrive sin saber que estaba infectado, no estaríamos ante un delito, salvo que pudiera acreditarse que se han producido daños por imprudencia grave, y que en cualquier caso sólo se castigaría como delito si se superase la cuantía de 80.000 euros, si bien en esta situación, el procedimiento sólo podría iniciarse a instancia de la persona agraviada o su representante, y aceptándose el perdón del ofendido y extinguiéndose entonces la responsabilidad penal, según establece el art. 267 CP.

Si tenemos en cuenta las diferentes teorías que nos pueden servir para explicar el lugar de comisión del delito, habrá que determinar mediante la Teoría de la actividad[33], el concreto lugar en el que se lleva a cabo la conducta típica; mediante la Teoría del resultado[34], el concreto lugar donde se produce el resultado y; en tercer

[31] Art. 10 CP: “Son delitos las acciones y omisiones dolosas o imprudentes penadas por la ley.”

[32] CEREZO MIR (1999:123): “El dolo, es decir, la conciencia y voluntad de la realización de los elementos objetivos del tipo, es también un elemento subjetivo de lo injusto de los delitos dolosos en nuestro Código.”

[33] COBO DEL ROSAL (1999:209 y ss.): ‘‘Como es sabido, existen tres criterios o teorías: a) Teoría de la actividad, según la cual el delito se entiende cometido donde el sujeto lleva a cabo externamente la conducta delictiva. b) Teoría del resultado, según la misma el delito se comete donde tiene lugar el resultado externo. c) Teoría de la ubicuidad, de acuerdo con ella, el delito se entiende cometido donde se lleva a cabo la actividad o se manifiesta el resultado”

[34] ARROYO ZAPATERO (2016:209): “Mientras que en los delitos de mera conducta el tipo solo requiere, bien una conducta activa (en los delitos activos) u omisiva (en los delitos omisivos), los

lugar, mediante el Principio[35] de la ubicuidad, ambos aspectos (conducta típica y resultado indistintamente) para evitar la impunidad de ciertos supuestos, y que en nuestro caso, tratándose de un virus informático, creado supuestamente en un tercer país y remitido desde ese país a España, debiendo determinarse si aplicaría en el primer país la teoría de la actividad y en el segundo la teoría del resultado.

La conducta típica, en la parte objetiva del tipo, representa un problema respecto de la imputación objetiva del resultado al sujeto o sujetos activos, pudiendo estar ante posibles delitos que requieren un resultado distinto a la acción de aquellos, bastando que se hayan o no llevado a cabo las conductas descritas en los tipos penales señalados para que se haya cumplido dicha parte objetiva.

En este supuesto, distinguir entre un delito de mera actividad, ex art. 264.ter y un delito de resultado, ex art. 197.bis, 264 y 264.bis, no resulta especialmente sencillo y ello es debido a varios aspectos: si entendemos que es suficiente la realización de una conducta tipificada como prohibida, en este caso la creación del virus mediante un programa informático para su propagación, podríamos encontrarnos ante un delito de mera actividad; pero si entendemos que el tipo señalado en nuestro ordenamiento penal exige no sólo acción, sino que para su consumación es necesaria también la producción de un resultado, cuál fue el bloqueo y la imposibilidad de acceso a los equipos informáticos y sus datos, o de sistemas informáticos, nos situamos entonces ante un delito o delitos de resultado, pudiendo haberse producido ambos sucesivamente.

IV.2.4. Objeto material.

El objeto material sería el objeto sobre el que recae físicamente la acción típica, pudiendo ser una persona o una cosa. Procede, como hemos señalado al describir a los sujetos pasivos, diferenciar por tanto entre estos y el objeto de la acción, aunque en ocasiones ambos coincidan, debiendo diferenciarlos a su vez del objeto jurídico del delito en relación con el bien jurídico protegido.

El objeto material no siempre se nos aparecerá en los delitos, dado que, en muchos casos, estos carecerán de aquél. Recordemos que nos hemos referido como bienes jurídicos, al patrimonio, a la intimidad, la seguridad de los datos o el orden socioeconómico.

En nuestro análisis, el objeto material podría distinguirse a su vez en dos elementos, los tangibles o físicos, como el propio ordenador o los servidores del sistema (que pueden resultar destruidos, dañados o inutilizados físicamente), y los programas o datos que contienen, que podríamos considerar como elementos lógicos intangibles, y que, en cualquier caso, el legislador ha querido proteger al referirse a ellos en las diferentes conductas tipificadas en el art. 264: las acciones de borrar (la destrucción lógica, que no física, de los datos), dañar (deterioro total o parcial de los mismos), alterar (perdida de su eficacia), suprimir (hacer desaparecer) o hacer inaccesibles (impedir el acceso lógico, como por ejemplo, modificando la clave de acceso, o

---

delitos de resultado requieren para su consumación que la acción o la omisión vaya seguida de la aparición de un resultado separable espacio-temporalmente de la conducta."

[35] Principio de la ubicuidad, definido en el acuerdo del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo, en su reunión del día 3 de febrero de 2005: "el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo".

eliminando los accesos a soportes físicos dentro del equipo o servidor, como por ejemplo un disco duro que contiene dichos datos o programas) datos informáticos, programas informáticos o documentos electrónicos ajenos de manera grave, esto es, que impida el funcionamiento de los mismos y que no puedan cumplir el fin para el que fueron creados, y que vienen a comportar un daño patrimonial por la necesidad de reparación o sustitución del referido objeto material sobre el que se hayan llevado a cabo dichas acciones.

En segundo lugar, tendríamos las conductas de sabotaje informático a las que se refiere el art. 264.bis cuando se refiere, en primer término, a la introducción o transmisión de datos en un sistema informático ajeno para obstaculizar el acceso o interrumpir el funcionamiento del mismo; y en segundo término, a la destrucción (el total funcionamiento), dañado (parcial), inutilización o sustitución de aquél, así como de un sistema telemático o de almacenamiento de información electrónica y cuyo objeto sería interferir de manera grave en el funcionamiento de dicho sistema informático. Cuando el legislador se refiere aquí al término "de manera grave", parece querer señalar una interrupción u obstaculización que impida necesariamente el funcionamiento del sistema informático.

Por tanto, en ambos casos, la gravedad de los daños tanto sobre los datos como sobre los sistemas informáticos (como desvalor del resultado), hemos de analizarla mediante la valoración de las pérdidas de las funcionalidades señaladas como objetos de los posibles delitos, identificando el daño y distinguiéndolo del posible perjuicio patrimonial ocasionado.

IV.3. El tipo subjetivo.

La parte subjetiva de los tipos penales señalados pueden referirse tanto al tipo doloso o al imprudente. Nuestro Ordenamiento penal señala que sólo serán punibles las acciones dolosas mientras que las imprudentes serán únicamente castigadas cuando expresamente lo disponga la ley[36]. De hecho, cuando el tipo delictivo no se refiere expresamente al elemento subjetivo, es que nos está queriendo decir que se exige el dolo, mientras que cuando el ordenamiento quiere castigar la imprudencia lo dice expresamente, como, por ejemplo, cuando el art. 267[37] señala que, en relación con el delito de daños, serán castigados los daños causados por imprudencia grave, si bien, requiere la denuncia previa de la persona agraviada, su representante legal o en su caso el Ministerio Fiscal.

Debemos analizar, pues, si nos encontramos ante una modalidad dolosa, de acción u omisión, imprudente, de acción u omisión, o ambas, valorando si el sujeto activo ha infringido una norma de cuidado ante un resultado previsible y evitable, pudiendo por tanto calificarse su conducta como imprudencia. Debemos comprobar si el tipo imprudente podría incardinarse conforme a lo señalado en el art. 12 CP, determinando a su vez la clase de imprudencia, pudiendo estar ante una imprudencia grave, leve o profesional.

El dolo consiste en primer lugar, en el conocimiento intelectual de la representación del resultado, es decir, el conocimiento de los elementos descriptivos y normativos

[36] Art. 12 CP

[37] Art. 267 CP: "Los daños causados por imprudencia grave en cuantía superior a 80.000 euros, serán castigados con la pena de multa de tres a nueve meses, atendiendo a la importancia de los mismos."

integrantes del tipo, y, en segundo lugar, la voluntad de realizar el tipo penal, esto es, la intención o aceptación de la producción de dicho resultado.

De los hechos analizados podrían desprenderse distintas conductas dolosas, apareciéndosele el delito al posible autor o autores del código del virus y su propagación, y los daños producidos, como resultados posibles, siendo un resultado causado por una o distintas acciones cuando éstas son condición sin la cuál no se producen dichos resultados.

Mediante el análisis del ataque, entendemos que la autoría y la conexión entre acción y resultado, se pudo producir cuando se hubiese adquirido o desarrollado para su uso, un programa informático concebido o adaptado para cometer alguno de los hechos mencionados, por ejemplo, un ransomware, código malicioso que permitiera acceder a totalidad o a una parte de un sistema de información, un programa (del inglés, botnet) que ejecutase la secuencia de puesta en marcha del mecanismo de bloqueo, aunque en muchos casos se requería para la puesta en marcha del código la participación imprudente o negligente del usuario, como por ejemplo, abriendo un correo electrónico que contuviera aquellos.

Respecto a la modalidad imprudente, el sujeto, como consecuencia de una conducta negligente, realiza el tipo objetivo sin haber querido su producción, pero habiendo causado un resultado, que lesionó o puso en peligro los bienes jurídicos señalados, pudiendo ser imputado objetivamente por dicha conducta imprudente. Por ello, debemos interpelarnos sobre tres posibles conductas imprudentes que pudiesen haberse dado.

La primera sería si podría resultar relevante penalmente la posible imprudencia grave de un supuesto autor del código malicioso o gusano que no tuvo la intención de propagarlo, infringiendo los deberes elementales que se le pueden exigir, o en su caso, si simplemente se trató de una imprudencia leve, desatendiendo las más elementales normas de cuidado, como, por ejemplo, al conectar un pendrive que contuviera el código a un equipo conectado a una red, dentro de un sistema informático.

La segunda sería si podría resultar relevante penalmente la posible imprudencia de Microsoft, como proveedor de sistemas informáticos de las empresas que utilizaban su sistema operativo por ser conocedores que un fallo de seguridad en su sistema posibilitaría un ataque con la magnitud de la que estamos tratando. Incluso la imprudencia profesional de sus empleados que hubiesen desarrollado el sistema operativo sin tener en cuenta los agujeros de seguridad en el mismo. Y en este mismo sentido, también podría ser relevante la posible falta de diligencia o, en su caso, posible imprudencia grave de los responsables y directores de sistemas de información y telecomunicaciones de las empresas afectadas, o incluso de los meros usuarios de equipos personales, por no haber aplicado e instalado el parche de seguridad que les fue remitido por Microsoft y que les convirtió en vulnerables ante el ataque del Wannacry. En este mismo sentido, nos referimos a las posibles actuaciones imprudentes de los sujetos pasivos, por una parte, con la imprudente decisión, de no actualizar sus sistemas operativos y por otra, a posibles actuaciones tendentes a la propagación del gusano de forma no volitiva o inconsciente, una vez que sus equipos resultaron infectados, como, por ejemplo, no apagando aquellos que estuvieran conectados a una red.

La tercera sería, si nos encontrásemos ante delitos imprudentes de resultado en la propagación del gusano, en los que sería preciso, que se haya producido un resultado material determinado, cuestión que parece no resultar controvertida puesto que resultaron infectados miles de equipos y sistemas de numerosos países, si bien, reiteramos la mención a la conducta que hubiesen tenido las víctimas del ataque, y que pudiesen haber incidido en la producción del resultado del delito, dado que existirían distintos elementos de riesgo que favoreciesen el ataque y la infección de equipos y sistemas informáticos, como visitar páginas de Internet susceptibles de contener el código malicioso del gusano, la apertura de correos electrónicos cuyo remitente es de dudoso origen o las descargas de programas infectados.

Por ello, a nuestro entender, en ambas cuestiones podemos estar ante conductas imprudentes tanto en el caso de Microsoft como de los responsables de sistemas de las empresas o servicios públicos, pero no dolosas, quedando excluidas del tipo penal en las circunstancias señaladas salvo si superan el límite económico señalado de 80.000 euros por los daños producidos y siempre que se iniciara el procedimiento penal a instancia de parte, si bien, podrían ser examinadas desde la perspectiva de la responsabilidad civil o laboral, en su caso.

Respecto al error del tipo, contenido en el art. 14.1 CP[38], se habría de analizar si cabría un error invencible, por faltar el elemento intelectual del dolo sobre los hechos constitutivos de cualquiera de las posibles infracciones penales excluyendo por tanto la responsabilidad criminal, o si, en caso de estar ante un error vencible, atenuarse dicha responsabilidad. Entendemos que no puede existir como tal, pese a que pudiera suponerse un desconocimiento o un conocimiento falso de alguno de los elementos de este. En el error, el sujeto no percibe de forma correcta la realidad de su conducta, pudiendo conocer alguno de sus elementos, pero no todos. El autor o autores persiguieron la realización de los delitos, dirigiendo las acciones a un fin, cual fue, tras acceder de forma no autorizada a los equipos y sistemas informáticos, bloquear el acceso a los datos contenidos en ellos y solicitar un pago para proceder a su desbloqueo, y en su caso, dañando o haciendo inaccesibles los datos, equipos y sistemas.

IV.4. La exclusión de la Antijuricidad.

La antijuricidad es otro de los requisitos que ha de cumplir la acción típica del ataque Wannacry, es decir, además de consistir en un conjunto de acciones descritas por la Ley, han de estar prohibidas. Se trata por tanto de analizar si nos encontramos ante un comportamiento contrario a nuestro Ordenamiento penal, mediante una puesta en peligro de los bienes jurídicos. Esto no significa que cualquier puesta en peligro de estos, como desvalor de cada uno de sus resultados, hayan de ser consideradas necesariamente conductas antijurídicas, sino que tan solo se producirá en aquellas acciones que se hallen desaprobadas, como desvalor de cada una de las acciones, por nuestro ordenamiento penal.

En virtud de lo anterior, debemos señalar que entre el desvalor de la acción como juicio negativo sobre el comportamiento del autor o autores de las conductas

[38] Art. 14.1 CP: “El error invencible sobre un hecho constitutivo de la infracción penal excluye la responsabilidad criminal. Si el error, atendidas las circunstancias del hecho y las personales del autor, fuera vencible, la infracción será castigada, en su caso, como imprudente.

realizadas desde la creación del Wannacry, y el desvalor del resultado como juicio negativo sobre la afectación producida a los distintos bienes jurídicos protegidos, ha de existir una conexión interna entre ambos, acciones y resultados. No obstante, podría concurrir alguna causa de justificación[39] que impidiese hablar de la existencia de un delito, excluyendo la antijuricidad de la conducta típica, pasando a convertirse en una acción sin relevancia para su análisis y calificación jurídico penal, en nuestro caso, teniendo en cuenta lo dispuesto en el art. 20 CP, que recoge como eximentes las situaciones de legítima defensa (art. 20.4º CP), el estado de necesidad (art. 20.5º CP), el cumplimiento de un deber o ejercicio de un derecho, oficio o cargo (art. 20.7º CP), como por ejemplo, si algún miembro de los servicios de seguridad del Estado, en cumplimiento de su deber, evitase la conducta delictiva del sujeto activo, introduciéndose a su vez en el equipo informático de este e impidiendo que pudiera realizar el tipo delictivo al destruir o bloquear sus propios códigos de acceso.

Ahora bien, ¿se admitiría que, para impedir una conducta delictiva, dicho agente de los servicios de seguridad del Estado actuase con la misma conducta, bajo el amparo de ese cumplimiento del deber? El Tribunal Supremo[40] ha señalado que es posible amparar esta causa de justificación siempre que el recurso a dicha acción resultara necesaria desde el punto de vista de los bienes jurídicos que se intentan proteger, que sea una acción proporcionada, y que concurra que sobre el sujeto activo cierto grado de resistencia o actitud peligrosa, siempre que exista un ánimo de cumplir con ese deber o ejercicio del oficio o cargo.

Por último, el consentimiento del ofendido podría entenderse como otra posible causa de justificación.

Las acciones ejecutadas el pasado 12 de mayo, contrarias al Ordenamiento penal, suponen un compendio de conductas típicas y prohibidas, que, tras haberse cometido, deben llevar aparejadas una pena. Podría ocurrir, como hemos señalado, que, pese a la prohibición por nuestro derecho, dichas conductas pudieran haber estado consentidas[41] por los sujetos pasivos al asumir que el hecho de tener instalado un sistema operativo en su equipo o sistema informático sin la protección adecuada, pudiera conllevar la posibilidad de ser objeto de una conducta lesiva por parte de un tercero, sujeto activo, ajeno a la propiedad de estos, mientras que no parece en este caso, que concurran algunas de las causas de exclusión señaladas en los apartados 4º, 5º o 7º del art. 20 CP.

IV.5. Culpabilidad.

Imputar un hecho típicamente antijurídico es atribuírselo a su autor o autores a modo de reproche desde el punto de vista del ordenamiento penal. El principio de culpabilidad se recoge en el art. 5 CP, que señala que "*no hay pena sin dolo o imprudencia".*

[39] CEREZO MIR (1999:189): "Toda acción comprendida en un tipo de lo injusto de los delitos de acción dolosos o imprudentes será antijurídica si no concurre una causa de justificación".
[40] STS, Sala de lo Penal, de 19 de junio de 1998, núm. 871/1998.
[41] MARTINEZ ESCAMILLA (2012:264): "Un supuesto particular viene dado por la figura del consentimiento, que, en general, actúa como elemento que excluye ya el tipo, pues el bien jurídico protegido es la libertad del sujeto o sólo se protege el bien jurídico si el sujeto así lo quiere."

Una vez determinado que han existido unas conductas humanas activas, típicas, descritas en el Código Penal y antijurídicas, hemos de analizar si las actuaciones llevadas a cabo en el ataque pueden ser imputables a una persona o personas físicas, o en su caso, a personas jurídicas, es decir, tenemos que determinar que el sujeto o sujetos activos sean imputables. Se determinaría por tanto la responsabilidad personal, desde la responsabilidad del hecho, con la exigencia del dolo o imprudencia y con la capacidad de atribuibilidad o imputación, requiriéndose aspectos que podrían concretarse en la imputabilidad, la exigibilidad y la conciencia de antijuricidad.

Para poder responsabilizar a los posibles autores del gusano de los hechos delictivos señalados, estos tienen que ser imputables, siendo la imputabilidad como hemos señalado, la capacidad de atribuir al autor o autores del ataque los hechos cometidos. Por ello, si no fueran imputables, no cabe proseguir examinando si las acciones señaladas son culpables.

Para determinar que las conductas típicas y antijurídicas son también culpables han de darse los elementos anteriores de imputabilidad y antijuricidad no habiendo de existir causas de exclusión, en cuanto causas que enervan la existencia del delito y que deberían ser probadas por los posibles autores.

Conocidos los sujetos activos, se habría de determinar si concurren causas de inimputabilidad, como la minoría de edad (art. 19 CP), la alteración psíquica o trastorno mental transitorio (art. 20.1º CP), estados de intoxicación (art. 20.2º) o alteración de la percepción (art. 20.3º).

Respecto al error de prohibición, contenido en el art. 14.3 CP[42], el sujeto o sujetos autores de la creación del código malicioso podrían desconocer o conocer falsamente la antijuricidad de sus conductas, si es que no hubiera sido creado para los fines relatados en el art. 264.ter lo que afectaría a la culpabilidad.

Parece obvio señalar que, dada la magnitud del ataque, los autores de la acción tenían consciencia y voluntad respecto al resultado, pudiendo castigarse los hechos delictivos al haber sido cometidos de modo doloso, es decir con conocimiento de su antijuricidad y con la voluntad de realizarlos, ya sea representándose sus consecuencias o, dado el caso, no haber hecho nada para evitar la propagación del virus, e incluso, aceptando un previsible resultado de la creación del código malicioso y de las acciones realizadas como consecuencia de su puesta en circulación, estando ante un dolo eventual. Pero, podríamos encontrarnos en el caso de haber sido cometidos por una persona enajenada sobre la que no cabría culpabilizar porque faltaría la esencia de este elemento, cual sería la comprensión de la ilicitud de los actos realizados y la posibilidad de poder evitar dicha acción. Podemos estar, en virtud de lo descrito, ante un supuesto en el que la persona que materializó las acciones descritas, típicas y antijurídicas, no se le podría imputar dichas acciones, tal y como nos señala el art. 20 CP[43]. En esta situación, en la cuál

[42] Art. 14.3 CP: "El error invencible sobre la ilicitud del hecho constitutivo de la infracción penal excluye la responsabilidad criminal. Si el error fuera vencible, se aplicará la pena inferior en uno o dos grados."

[43] Art. 20 CP: "Están exentos de responsabilidad criminal: 1.º El que al tiempo de cometer la infracción penal, a causa de cualquier anomalía o alteración psíquica, no pueda comprender la ilicitud del hecho o actuar conforme a esa comprensión."

nos encontramos ante una conducta típica y antijurídica pero no culpable, podemos señalar que el sujeto no respondería penalmente pero sí civilmente conforme a lo dispuesto en los artículos 118 y 119 CP.

IV.6. Iter criminis.

En lo analizado hasta el momento, hemos determinado que se han producido posibles conductas dolosas e incluso conductas imprudentes, que derivaban en un resultado por lo que a partir de ahora debemos establecer si los sujetos activos deben responder penalmente por los delitos que hubieran podido quedar consumados y acreditados.

El *iter criminis,* o camino del delito[44], se refiere a los distintos momentos temporales que se producen en el delito, desde el momento que la idealización de este es concebida y se produce materialmente, como por ejemplo en nuestro caso, con la creación de un código malicioso que pueda efectivamente propagarse y causar un daño informático, hasta que el mismo se lleva a cabo de modo completo, introduciéndose de forma ilícita en un equipo o sistema informático.

Procedería determinar, tras la investigación judicial, si las infracciones señaladas se han consumado, en relación con el análisis posterior de las posibles penas aplicables, teniendo en cuenta además los elementos de decisión, actos preparatorios punibles (art. 17 y 18 CP) y actos ejecutivos, distinguiendo entre tentativas (art. 15, 16 y 62 CP), desistimiento (art. 16.2 CP) o consumación (art. 15.1 CP). En cualquier caso, una vez acreditada la consumación de los distintos delitos, hemos de señalar que las fases anteriores quedarían absorbidas por las ulteriores, en virtud de no producir una doble sanción por las mismas conductas.

En nuestro caso, la consumación del delito se produce en primer lugar, con la creación del programa o código malicioso. En segundo lugar, con la distribución del gusano, y en tercer lugar, una vez que el autor o autores acceden de forma no autorizada a los equipos y sistemas informáticos, bloqueando el acceso a los datos contenidos en ellos y solicitando un pago de un rescate para proceder a su desbloqueo, y en su caso, como hemos señalado, dañando o haciendo inaccesibles los datos, equipos y sistemas.

Existe y se utiliza un nexo común y global a todos ellos, tal que sería cualquier sistema o equipo informático que está conectado a internet o a una red comunicada entre si que se ve afectado por la consumación del tipo delictivo.

IV.7. Autoría y participación.

El art. 61 CP señala que *"cuando la Ley establece una pena, se entiende que la impone a los autores de la infracción consumada*." La autoría existirá por tanto cuando se realice la conducta típica, antijurídica y culpable, entendiéndose consumada, distinguiendo nuestro ordenamiento penal entre personas criminalmente responsables de los delitos, en los sujetos activos, entre autor,

[44] MARTINEZ ESCAMILLA (2012:196): "Este conjunto de fases o etapas de desarrollo del delito es lo que se denomina *iter criminis* (camino hacia el delito)."

coautor y autor mediato, conforme a lo señalado en el art. 27 CP, pudiendo realizar el hecho por sí solos, conjuntamente o por medio de otro del que se sirven como instrumento[45].

Por otra parte, nuestro código penal estable otras formas de participación como el posible inductor (art. 28.a CP), el cooperador necesario (art. 28.b CP), cómplices (art. 29 CP), o, la participación intentada (art. 17 CP).

Cabe reseñar, que cuando existan circunstancias agravantes o atenuantes que sean de aplicación sobre cualquier causa de naturaleza personal, sólo se aplicarán sobre la responsabilidad de aquellos sobre los que concurran[46].

IV.7.1. La problemática de los sujetos activos en la autoría del ataque.

Como personas criminalmente responsables de los delitos en el ataque debemos distinguir, por tanto, entre autores, supuestamente creadores del código malicioso, respecto al delito de mera actividad y, aquellos que intencionadamente lo pudieran haber supuestamente distribuido y, sus posibles cómplices, conforme a lo que ya hemos señalado en el art. 27 CP, pudiendo realizar el hecho por sí solos, conjuntamente o por medio de otro del que se sirven como instrumento. Serían supuestamente aquél o aquellos que crearon el Wannacry, programa o código malicioso, por una parte, o siendo los mismos o distintos, quién o quienes supuestamente lanzaron el ataque y la conducta delictiva de propagación de este. También resultarían ser supuestos autores, aquellos quiénes de manera no autorizada se hubieran introducido en los equipos o sistemas informáticos, o quiénes, supuestamente, de forma remota hubiesen bloqueado los mismos o los datos contenidos en ellos, o quienes hubieran dañado datos, programas, equipos o sistemas.

Tras la reforma operada por la LO 1/2015 pueden ser sujetos activos tanto las personas físicas como jurídicas, conforme a lo señalado en el art. 31.bis CP. Conforme a lo relatado en el ataque pueden haber participado personas jurídicas u organismos públicos. En el caso de referencia, podría ser relevante en cuanto a la autoría y participación, si es que pudiera considerarse que se tratara de un delito especial dado el caso que hubiese acreditado la intervención de sujetos cualificados, junto a otros sujetos no cualificados. Pero como hemos señalado, las hipótesis sobre la posible autoría, nos conduce de forma no acreditada, según la fuente de la noticia, a distintos organismos gubernamentales de terceros países.

Desconocemos por tanto en este caso quién o quiénes fueron los sujetos activos del ataque, existiendo distintas teorías sobre la autoría de este y por tanto desconocemos la autoría. La investigación de las posibilidades de creación y difusión del gusano Wannacry, llevan a suponer distintas posibilidades sobre la posible autoría[47]: por un parte, al Gobierno de Corea del Norte y por otra, quién atribuye la posible autoría a una derivación de una aplicación creada por la Agencia

[45] Art. 28 CP
[46] Art. 65 CP
[47] https://computerhoy.com/noticias/software/corea-del-norte-fue-responsable-wannacry-segun-nsa-63680. “Ahora se ha conocido un informe elaborado por el Departamento de Seguridad Nacional y la Oficina Federal de Investigaciones de Estados Unidos que vincula al gobierno de Corea del Norte con la creación del malware WannaCry.”

Nacional de Seguridad (NSA) estadounidense[48]; autoría que a fecha de redacción del presente trabajo sigue sin averiguarse.

Si nos atenemos a lo señalado por el art. 17.1 CP debería determinarse si existe conspiración[49] en caso de establecer que dos o más personas hayan concertado la ejecución y decisión tanto en la creación del código, como en su distribución, así como en la conducta típica de exigir un rescate por el desbloqueo de los datos o equipos.

Esta circunstancia tiene especial relevancia, en el sentido de que, conforme a lo establecido en el art. 779 LECrim[50], una vez practicadas las diligencias pertinentes, en caso de haber iniciado las actuaciones judiciales de persecución de las conductas penales, el Juez adoptará mediante auto, aun estimando que los hechos pudieran ser constitutivos de delito, al no haberse determinado autor conocido, acordará el sobreseimiento provisional y ordenará el archivo de la causa.

IV.7.2. La problemática de la aplicación del Principio de Territorialidad y el tiempo de las conductas delictivas.

La cuestión relativa a la relación entre la autoría y el lugar del ataque inicial ha de resolverse mediante el Art. 23.1[51] LOPJ, que establece que sólo podemos perseguir en España por los delitos cometidos en España, por personas que estén en España, por personas, cuando sea español quién lo comete o quién lo sufre. Y en el supuesto que nos atañe, habiendo sido empresas españolas entre otras y sus usuarios, entre otras, las que han sido atacadas, debemos aplicar el Principio de Territorialidad, en virtud del cual, nuestro ordenamiento penal será de aplicación a todos los delitos cometidos por aquellos que se hallen en territorio español.[52] Según este principio, España sería competente para enjuiciar estos delitos, si es que fue aquí donde se llevó a cabo y realizó la actividad antijurídica y/o se produjo el resultado. No resulta por tanto cuestión baladí, la persecución de los posibles delitos del ataque ante la dificultad de determinar, como hemos señalado, el lugar de comisión, teniendo en consideración que la acción puede llevarse a cabo desde un lugar o múltiples lugares no identificados, a través de diferente medios o dispositivos, en distintos formatos o plataformas, cuyas direcciones IP pueden estar a su vez ubicadas en servidores de distintos países, con los que España puede tener o no acuerdos internacionales de cooperación en materia penal. Y de nuevo

[48] https://elpais.com/tecnologia/2017/05/15/actualidad/1494835268_125044.html. "Se cree que WannaCry está basado en EternalBlue, aplicación desarrollada por la Agencia Nacional de Seguridad (NSA) estadounidense para atacar ordenadores que utilicen el sistema operativo Microsoft Windows, para lo que aprovecha los agujeros de seguridad".

[49] STS 1994/2002, Sala de lo Penal, de 29 de noviembre (Rec. 1621/2001): “La conspiración existe, según la ley, «cuando dos o más personas se concierten para la ejecución de un delito y resuelven ejecutarlo» (art. 17-1º CP). Nos hallamos, pues, ante la denominada «coautoría anticipada», en la que se prevé la intervención de todos los conspiradores en la realización material del hecho delictivo, sea cual fuere el cometido o la parte del plan acordado que les haya tocado ejecutar a cada uno de los concertados.

[50] Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal, publicado en GACETA de 17 de septiembre de 1882.

[51] Art. 23.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial: «En el orden penal corresponderá a la jurisdicción española el conocimiento de las causas por delitos y faltas cometidos en territorio español o cometidos a bordo de buques o aeronaves españoles, sin perjuicio de lo previsto en los tratados internaciones en los que España sea parte»

[52] Art. 8.1 CC.

adquieren condición relevante, las notorias dificultades en la averiguación y comprobación de los hechos producidos mediante el ataque del gusano Wannacry, pues puede resultar relativamente sencillo para los autores ocultarse mediante redes que permiten su encriptación, pseudonimización o codificación, incluso en equipos informáticos de personas físicas o jurídicas que desconocen que están siendo utilizados para llevar a cabo el ciberataque criminal.

La Sala II del Tribunal Supremo vino a establecer que el delito que se haya cometido desde un lugar ignoto o indeterminado y con efectos en distintos lugares, si identificados, puede ser perseguido judicialmente en todos y cada uno de ellos[53].

El Wannacry, en primer lugar, ya sea considerado desde el punto de vista de los posibles daños informáticos como desde cualquier otro que derive a distintos tipos de actos delictivos realizados y relacionados con los equipos o sistemas informáticos, se caracteriza probablemente, al no estar investigado ni acreditado, por haberse llevado a cabo supuestamente de forma remota, por lo que inicialmente debemos resolver la problemática cuestión de determinar su origen así como el tiempo del ataque, desconociéndose si se llevó a cabo con un botnet que pudiera estar programado para su ejecución en momentos posteriores a los de su instalación en los equipos o sistemas informáticos, siendo este problema sustancial y decisivo para poder comenzar la investigación y la persecución policial y judicial; e incluso, que dicho botnet estuviese programado para ejecutar una orden automática de engaño para hacer creer al sujeto pasivo que debía pagar una cantidad de rescate que posteriormente se depositaría en algún lugar de la web mediante un pago en criptomoneda electrónica.

En segundo lugar, nos encontramos con otro aspecto de difícil respuesta jurídica, y es que podemos estar ante una pluralidad de posibles atacantes ubicados en diferentes y desconocidos lugares del planeta, que pueden haber llevado a cabo la acción de forma dolosa o imprudente, siendo necesario identificar al posible creador o creadores, su organizador u organizadores, y/o, a quiénes han contribuido a su propagación de forma consciente e intencionada.

IV.8. Las consecuencias jurídicas derivadas del delito: Punibilidad.

Tras el análisis anterior de los elementos básicos del delito, acción, tipicidad, antijuridicidad y culpabilidad, hemos de referirnos a un siguiente aspecto, cuál es la punibilidad, como posibilidad de imponer penas, es decir, posibilitar el castigo de las conductas típicas y cómo deben ser aquellas[54]. Los delitos por las acciones señaladas en la creación del código y posterior ataque Wannacry requerirían la imposición de penas, respetando la debida proporción con la gravedad de los hechos cometidos. Incluso podemos estar ante una situación en la que pese a probarse la autoría de su autor o autores, podrían existir razones que lo impidieran.

[53] Acuerdo del Pleno no jurisdiccional de la Sala II del Tribunal Supremo de 3 de febrero de 2005.

[54] GIMBERNAT (2016:19): “Pero estas funciones del Derecho penal sólo nos indican cuáles son los fines que persigue, pero no nos dicen nada aún ni sobre su contenido, es decir: sobre cuáles son aquellas conductas que deben ser tipificadas como delito, ni tampoco sobre cómo de ser la consecuencia jurídica que el legislador vincula a aquél, es decir, sobre cómo debe ser la pena”.

Nos referimos a aquellos supuestos en los que la acción del ataque, antijurídica y culpable, pudiera no tener la consideración de delito, por aparecerse concretas condiciones objetivas de punibilidad o bien, que se dieran causas absolutorias que provocaran la desaparición de la punibilidad de dichas conductas típicas, antijurídicas y culpables, como, por ejemplo, que el autor o autores fuesen menores de edad, conforme a lo que señala el art. 19 CP[55], o como hemos señalado anteriormente, la enajenación del autor, conforme a lo referido en el art. 20 CP.

Las penas previstas para los autores de las acciones típicas de vulneración[56] de medidas de seguridad establecidas para impedirlo y sin estar debidamente autorizado, accediendo o facilitando a otro el acceso al conjunto de un sistema de información o a parte de este, o se mantenga en él, en contra de la voluntad de quién tenga el legítimo derecho de excluirlo, serán de seis meses a dos años.

Las penas previstas por el Código Penal para las acciones típicas de los daños informáticos regulados por los artículos 264, 264.bis y 264.ter son la de prisión de 6 meses a 3 años en los supuestos de daños y de obstaculización o interrupción del funcionamiento de un sistema informático ajeno.

Respecto de las formas agravadas, conforme a lo previsto para el delito contenido en el art. 264 CP, la pena de prisión de 2 a 5 años y multa del tanto al décuplo del perjuicio ocasionado, si se hubiese cometido en el marco de una organización criminal, cuestión que en el caso estudiado desconocemos. Si bien, lo que si resultaría acreditado sería el hecho de haber ocasionado daños de especial gravedad, habiendo también afectado a un número elevado de sistemas informáticos, perjudicado el funcionamiento de servicios públicos esenciales como pudieran ser considerados los servicios de salud o las telecomunicaciones, o habiéndose llevado a cabo mediante alguno de los medios relacionados en el art. 264.ter. Respecto a las acciones señaladas en el análisis conforme al art. 264.bis, se impondría las penas en su mitad superior, alcanzándose la superior en grado, ya que los hechos perjudicaron de forma relevante la actividad normal de distintas empresas, como el caso de Telefónica, pudiendo imponerse una pena de prisión de 3 a 8 años y multa del triple al décuplo del perjuicio ocasionado, por haberse producido cualquiera de las circunstancias referidas en el art. 264.2, e imponiéndose en todas las penas en su mitad superior, si se acreditara que los hechos se hubiesen llevado a cabo mediante la utilización ilícita de datos personales obtenidos mediante la acción del gusano Wannacry.

Respecto a los delitos se hubieran cometido por una o varias personas jurídicas, hemos de proceder a determinar su responsabilidad penal, teniendo en cuenta los requisitos de las conductas o las propias excepciones en relación con lo señalado en el art. 31bis para valorar si procede o no atribuirles aquellos, así como las reglas de determinación, art. 66bis CP y las posibles penas aplicables conforme a los dispuesto en el art. 33. CP en relación con los arts. 50 y 52 CP; así como los aspectos de derivados de su responsabilidad civil y las consecuencias accesorias, según lo dispuesto en los arts. 116.3 y 129 CP respectivamente. Según lo dispuesto en el art. 264.quáter, a las personas jurídicas responsables de la autoría se les

[55] Art. 19 CP: “Los menores de 18 años no serán responsables criminalmente con arreglo a este código. Cuando un menor de dicha edad comenta un hecho delictivo podrá ser responsable con arreglo a lo dispuesto en la Ley que regule la responsabilidad penal de menor.”
[56] Art. 197.bis CP

impondría una 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, o multa de uno a tres años o del triple a ocho veces el valor de perjuicio causado, si resultase una cantidad superior, en el resto de los casos.

IV.9. La prescripción de los delitos y penas.

Los distintos plazos de tiempo de la prescripción[57] estarán en función de la gravedad de los delitos y las penas. En este sentido, la Jurisprudencia ha determinado que el paso del tiempo pueda llevar a la pérdida de la posibilidad de condenar por una infracción penal producida o la posibilidad de aplicar una pena a esta, ya que, según lo dispuesto en el art. 9.3 CE[58], el castigo sería desproporcionado.

Nuestro ordenamiento penal recoge las posibles causas de extinción de la responsabilidad criminal, y particularmente respecto de la fecha de prescripción de los delitos en los arts. 130 a 135 CP.

Respecto de las posibles prescripciones de delitos y penas que pudieran aplicarse al ataque, podríamos señalar que los posibles delitos prescribirían a los 10 años en el supuesto que se estableciera una pena de prisión entre 5 y 10 años, o a los 5 años, en el caso de prisión hasta 5 años.

Las reglas de interrupción de la prescripción vendrían dadas por resolución judicial motivada que atribuyera la presunta participación a una o varias personas físicas o jurídicas, o por la presentación de denuncias o querellas, suspendiendo en este caso el cómputo por 6 meses, cuestiones ambas que no nos consta que se han producido en este caso.

IV.10. Concursos.

Tomando en consideración lo dispuesto en los arts. 73 a 79 CP, hemos de valorar las reglas especiales para la determinación de las penas en aquellos casos de unidad y pluralidad de delitos, así como posibles supuestos de continuidad de estos, mediante los criterios establecidos de acumulación material, es decir, la suma de las penas correspondientes a todos los delitos, y la acumulación jurídica por agravación de la pena correspondiente a la infracción más grave hasta un límite máximo.

En relación con lo estudiado se nos podrían aparecer distintas figuras relativas al concurso tal y como dispone nuestro Código penal, y como hemos podido analizar, también en esta cuestión es complejo determinar si junto al delito de daños informáticos del art. 264 y ss. CP podrían aparecer en paralelo o derivadas del delito

---

[57] STC 37/2010 de 19 de julio: "El establecimiento de un plazo de prescripción de los delitos y faltas no obedece a la voluntad de limitar temporalmente el ejercicio de la acción penal de denunciantes y querellantes (configuración procesal de la prescripción), sino a la voluntad inequívocamente expresada por el legislador penal de limitar temporalmente el ejercicio del *ius puniendi* por parte del Estado en atención a la consideración de que el simple transcurso del tiempo disminuye las necesidades de respuesta penal (configuración material de la prescripción)"

[58] Art. 9.3 CE: "La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos."

recogido en el 197.bis otras figuras que determinaran la existencia de las posibles figuras del concurso real, medial o ideal de delitos o en su caso, del concurso de leyes. Se nos aparece la situación en la que un conjunto o pluralidad de hechos constituyen un concurso real por producir una pluralidad de delitos, debiendo acudir a la figura de la unidad de acción.

Podría ocurrir que con la conducta típica que produce el daño en el equipo o sistema informático se incurra a la vez en el descubrimiento de secretos, conforme a lo dispuesto en el art. 197 CP. Sería posible que, ateniéndonos a la redacción del art. 264.1 en relación con el 264.2 CP, podamos encontrar dos o más delitos a través de una sola conducta típica, esto es, por una parte, el daño grave y sin autorización a los datos y por otra, el bloqueo o interrupción de manera grave del acceso a los mismos, si bien para cometer el segundo se habría de haber producido el primero.

Señalado lo anterior, también podríamos encontrarnos ante un posible concurso real por constituir una pluralidad de delitos, o medial de delitos en el que una primera acción, cual es la creación del código malicioso (art. 264.ter) constituye dos o más delitos, el acceso no autorizado a los equipos (art. 197.bis) y un delito de daños informáticos por el bloqueo de datos o interrupción del funcionamiento de los equipos que los contienen (art. 264.bis) y finalmente un posible delito de estafa (art. 248 CP) pero nada impide que pudiésemos considerar que estamos ante situaciones que nos lleven a considerar cualquiera de ellos, una vez hubiésemos determinado todos los aspectos en la instrucción judicial.

La dificultad residirá por tanto en poder establecer o separar las unidades de acción, teniendo en cuenta además que el problema de la ejecución temporal del delito en tanto que no conocemos el inicio, su programación, ni si las distintas acciones se han llevado a cabo en un mismo momento en el tiempo y si el autor o autores han llevado a cabo una o varias acciones, aunque del análisis del supuesto, en nuestra opinión procederíamos a aplicar el concurso real en primer lugar, sin obviar que los apartados 3 y 4 del art. 197 CP podrían determinar que nos encontrásemos ante un concurso medial en el que el daño se produce tras haber accedido a los datos habiendo vulnerado las contraseñas de acceso y produciendo el daño a los mismos a continuación.

Respecto al posible supuesto de estafa[59], en el caso de acreditarse que se produce un engaño para hacer creer al sujeto pasivo que el acceso al equipo o a los datos no podría revertirse sino se produce el pago de 300 dólares, encontramos aquí de nuevo la dificultad de determinar si es uno o varios sujetos activos autores de la conducta, y si podemos estar ante un delito continuado, en el caso de que sea un único autor el que cause el engaño, de la cuantía inferior a 400 euros en cada uno de ellos. En el supuesto de entender que el delito se produce en una totalidad de sujetos pasivos, podría castigarse con una pena superior en uno o dos grados a la ordinaria (art.74.2 CP).

Además de lo señalado, la función del gusano Wannacry, y ahí radica otro de sus peligros, es que mediante el mismo, podría dar acceso al atacante a datos del

[59] Art. 248 CP: "1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno."

usuario[60] como, por ejemplo, al sistema operativo utilizado, las páginas visitadas, el tiempo que se ha estado en las mismas, descargas realizadas, etc., e incluso puede llegar a transferir datos privados y personales como direcciones de correo electrónico, direcciones IP y aquella a la que se realiza la conexión a Internet con su nombre de usuario y contraseña, etc. con los que luego estafar a otras personas; siendo razón por la que se podría considerar al autor de la conducta como reo de estafa. En dicho tipo subsisten los mismos elementos configuración del delito de estafa tradicional si bien el engaño no se va a realizar en el ámbito de una relación personal sino a través de una manipulación informática.

Asimismo, el tipo nos habla no solo de manipulación informática sino de artificio semejante, por lo que se admitirán distintas modalidades de comisión tales como la creación de órdenes de pago o transferencias o bien a través de manipulaciones de entrada y salida de datos (o actuando sobre el mismo programa) en virtud de los cuales la máquina va a realizar su función mecánica propia.

Pese a lo anterior, en el caso del ataque, no ha transcendido conforme a lo estudiado, que se hayan producido conductas dirigidas a la comisión dolosa posterior del delito de estafa.

Es relevante, además, la posibilidad de encontrarnos, conforme a lo dispuesto en el art. 74.1 CP, ante un posible resultado múltiple que afecta a una pluralidad de afectados y constituyendo, por tanto, un supuesto delito continuado, o un delito masa, si nos atenemos a lo señalado por el art. 74.2 CP, debiendo considerar además que nos encontramos ante una enorme magnitud de sujetos pasivos indeterminados por no haberse tramitado las correspondientes denuncias penales por la práctica totalidad de ellos. Recordemos aquí que el ataque afectó a más de 250.000 equipos, así como a diferentes empresas, organizaciones, servicios y usuarios. El ataque inicial, con una sola acción produjo múltiples conductas típicas. Esto incrementaría las posibles penas aplicables hasta en dos grados.

V. CONCLUSIONES

Actualmente la sociedad está inmersa en un entorno completamente digital, en el que asistimos a un ritmo frenético y día tras día al nacimiento de tecnologías disruptivas y en paralelo, nuevas conductas delictivas. Como hemos visto a lo largo del trabajo, este progreso tecnológico está considerado, además de la principal vía de desarrollo de nuestra sociedad, como un riesgo en si mismo contra los derechos de las personas y las organizaciones, y el derecho a la protección de sus datos, equipos y sistemas informáticos. No debemos considerar que el riesgo y el déficit legal y jurisprudencial provenga únicamente del progreso técnico en si, sino que es el resultado de unos procesos legislativos no adaptados a la realidad evolutiva.

Durante esta revolución tecnológica, no podemos destacar de forma aislada los aspectos beneficiosos de la innovación, dado que a la par han aparecido y crecido los ciberdelitos, que han requerido una respuesta, en ocasiones tardía, por parte del legislador a nivel europeo, para perseguir toda clase de conductas ilícitas que con el transcurso de los años se han ido convirtiendo en nuevos tipos penales concebidos

[60] Art. 248.2.b): " Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo".

para atajar aquellas, que han afectado a bienes jurídicos individuales y colectivos. Las normas jurídicas no han sufrido tal revolución, o al menos no al mismo ritmo que las nuevas tecnologías, lo que ha venido provocando en muchas ocasiones que nos veamos inmersos en un lapso sin marco jurídico adecuado que aplicar a todas estas novedosas y vertiginosas situaciones, si bien es cierto que desde la ratificación por España del contenido del Convenio Europeo de Ciberdelincuencia hasta la última reforma operada por la LO 1/2015 se han introducido cambios sustanciales de especial relevancia, que en parte han podido quizás ayudar a combatir estos denominados ciberdelitos.

Los piratas cibernéticos de cualquier lugar del mundo son capaces de lanzar ataques globales. En el caso del Wannacry, es probable que los piratas informáticos pusieran sus ojos en objetivos más lucrativos. Cuando se extendió en mayo de 2017 descubrimos que el ramsonware se puede haber convertido en la principal amenaza cibernética en todo el mundo, incluso en una nueva forma bélica, ya que nunca se había visto nada a dicha escala.

Por tanto, en primer lugar, debemos desechar por otra parte la idealización del pirata informático individual, que casi a modo de simple diversión trata de saltar las barreras de seguridad de un equipo, sino que debemos, a nuestro parecer, enfocarnos en la persecución de empresas y organizaciones, incluso en la órbita de algún gobierno, que son verdaderamente quiénes llevan a cabo los ataques en busca de las vulnerabilidades y agujeros de seguridad. La respuesta de nuestro país o de cualquier otro a un ciberataque no debería ser otro ciberataque, primero porque se desconoce probablemente ante quién se ha de responder al ataque sufrido y por tanto sería una medida altamente ineficaz, y en segundo término, y lo que es más relevante desde nuestro punto de vista, es que el propio Estado vulneraría supuestamente nuestro Ordenamiento penal y el marco normativo europeo que hemos adoptado.

En segundo lugar, en la evolución de nuestro Derecho penal se vino sosteniendo que sólo las personas físicas podían ser sujetos activos de la acción típica. Pero el legislador español, mediante la Ley Orgánica 5/2010 introdujo una modificación sustancial relevante al considerar a las personas jurídicas como sujetos que pueden cometer delitos. En este sentido, cabe señalar que en el ataque al igual que en las conductas enumeradas, podemos estar ante un delito cometido por personas físicas o por personas jurídicas tal y como se señala en el art. 264.quaterCP, e incluso como hemos referido, pudiendo estar ante una acción típica llevada por un objeto inanimado cuál sería una máquina o artefacto informático auto programable.

En tercer lugar, un aspecto relevante resulta ser el efecto colateral que se produce en la víctima del ataque, cuando tratándose de una empresa o incluso un particular no procede a denuncia alguna o investigación pública de los hechos, para así minimizar aspectos relativos al impacto en su responsabilidad social corporativa o ante un posible deterioro de su imagen que pueda afectar a la continuidad del negocio.

En cuarto lugar, nos hemos adentrado también, en la no fácil cuestión de la determinación del bien jurídico protegido en tanto en cuanto que, a diferencia del delito general de daños, en los artículos 264 y ss. no se hace referencia a una cuantía patrimonial, salvo en el art. 267, sino que se hace referencia a algo mucho más inconcreto y en casos intangible como sería la seguridad informática o . Y aquí

nos encontraríamos con otro aspecto a analizar tanto desde la óptica del ordenamiento jurídico como desde el punto de vista técnico dado que la evolución tecnológica provee a su vez una serie de elementos de protección de los equipos informáticos y medidas de seguridad que supuestamente protegen la intimidad y los accesos no deseados a los equipos y sistemas, tales como antivirus o herramientas específicas que impedirían dichos accesos, estando todo este conjunto de medidas técnicas a disposición del usuario que podrá hacer uso o acceder a las mismas por decisión propia o por razones económicas para garantizar una autoprotección frente a la amenaza. Con esto se puede poner de manifiesto que el propio usuario podría estar incurriendo en una imprudencia o situarse ante un riesgo tolerado.

En quinto lugar, es necesario reflejar que la complejidad del conocimiento de las medidas técnicas exige una preparación en el ámbito tecnológico y que requerirá a futuro una especialización en los tribunales para poder así otorgar una respuesta penal satisfactoria a las conductas delictivas actuales y futuras.

Para finalizar, debemos resaltar que en el mundo global en el que nos encontramos es absolutamente necesaria la cooperación y la armonización de normas penales no sólo en el ámbito de la Unión Europea sino en un ámbito mundial para poder perseguir las conductas delictivas en cualquier lugar del planeta a sabiendas que el delito puede iniciarse en un país, la propagación en un tercero y el resultado final en otro distinto. Requerirá a su vez la implicación de los operadores de telecomunicaciones ya que son ellos quienes deben poner a disposición de los investigadores policiales y judiciales el acceso a los datos registrados que puedan evidenciar algún tipo de indicio o prueba que permita identificar a los autores materiales de las referidas conductas. Por ello, debemos convenir, que habría de ser la ONU, mediante un convenio firmado por todos los países, quién se convirtiera de forma efectiva en el organismo que armonizara la implantación de un mecanismo o procedimiento vinculante para perseguir y poder castigar las conductas referidas en cualquier lugar del planeta y, a su vez, poder así, con las pruebas que se puedan obtener en distintos países, establecer un procedimiento judicial basado en el principio de jurisdicción universal, cuestión por otra parte, más bien utópica dados los antecedentes que hemos vivido en los últimos años.

VI. BIBLIOGRAFÍA Y WEBGRAFÍA

AGUILERA LÓPEZ, P. (2010), *Seguridad Informática*, 1ª edición, Pozuelo de Alarcón, Editorial Editex, pág. 102.

BERDUGO GÓMEZ DE LA TORRE, I. - ARROYO ZAPATERO, L. (2016), Curso de *Derecho Penal*. *Parte General*, 3ª edición, Masnou, Ediciones Experiencia, págs. 98, 209

CASAS HERRER, E. (2017), *La red oscura: en las sombras de Internet: el cibermiedo y la persecución de los delitos tecnológicos*, 1ª edición, Madrid, La Esfera de los Libros, pág. 160.

CEREZO MIR, J. (1999), *Curso de Derecho Penal español*. *Parte Especial*, 6ª edición, Madrid, Tecnos, págs. 19, 123, 151, 152, 189.

COBO DEL ROSAL, M. – VIVES ANTÓN, T. S. (1999), *Derecho penal. Parte general*, Tirant lo Blanch, Valencia, pág. 209.

ESPAÑA BOQUERA, M.C. (2003), *Servicios Avanzados de Telecomunicación*, 1ª edición, Madrid, Ediciones Díaz de Santos, pág. 180.

FERNÁNDEZ APARICIO, J.M. (1998), *Los antecedentes penales. Efectos: la nueva reincidencia en el Código Penal*. La Ley: Revista jurídica española de doctrina y bibliografía, Nº 5, pp. 1740-1745.

GALÁN MUÑOZ, A. (2006), *Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática".* Revista de Derecho y proceso penal, nº 15, p. 30.

GARCÍA VALDÉS, C.-MESTRE DELGADO, E.-FIGUEROA NAVARRO, C. (2015), *Lecciones de Derecho Penal*, 2ª edición, Madrid, Edisofer, págs. 151-152.

GIMBERNAT ORDEIG, E. (1990), *Estudios de Derecho Penal*, 3ª edición, Madrid, Editorial Tecnos, pág. 160.

GIMBERNAT ORDEIG, E. (2016), *Código Penal*, 23ª edición, Madrid, Editorial Tecnos, pág. 19.

JARA, H., PACHECO, F. G. (2012), *Ethical Hacking 2.0*, 1ª edición, Buenos Aires, coedición Fox Andina y Dálaga, pág. 300.

LESSIG, L. (2001), *El código y otras leyes del ciberespacio*, 1ª edición, Barcelona, Taurus, pág. 6.

MARTÍNEZ ESCAMILLA, M.-MARTÍN LORENZO, M.-VALLE MARISCAL DE GANTE, M. (2012), *Derecho Penal. Introducción Teoría Jurídica del delito*, Madrid, Universidad Complutense, págs. 87, 196, 264.

MUÑOZ CONDE, F. (2015), *Derecho Penal. Parte Especial*, 20ª edición, Valencia, Tirant Lo Blanch.

SUÑE LLINÁS, E. (2002), *Tratado de Derecho Informático Volumen I*, 1ª edición,

Madrid, Editorial Complutense, pág. 3.

TORRES VIÑALS, J. (2011), *Derecho Penal. Parte Especial*, 1ª edición, Barcelona, Libros de cabecera, pág. 84

Webgrafía

https://elpais.com/tecnologia/2017/05/16/actualidad/1494927608_413489.html.Fecha de última consulta 07/06/18.

http://dle.rae.es/?id=LY8zQy3. Fecha de última consulta 07/06/18.

http://dle.rae.es/?id=T8ktrp2. Fecha última consulta 07/06/18.

https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/; fecha de última consulta 07/06/18.

https://blog.avast.com/es/ransomware-telefonica-hospitales. Fecha de última consulta 07/06/18.

CCN – CERT: Comunicado publicado el 12 de mayo de 2017 a través de su página web https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html. Fecha de última consulta 07/06/18.

https://computerhoy.com/noticias/software/corea-del-norte-fue-responsable-wannacry-segun-nsa-63680. Fecha de última consulta 07/06/18.

https://www.boe.es/doue/2005/069/L00067-00071.pdf. Fecha de última consulta 07/06/18.

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al33193. Fecha de última consulta 07/06/18.

https://computerhoy.com/noticias/software/corea-del-norte-fue-responsable-wannacry-segun-nsa-63680. Fecha de última consulta 07/06/18.

VII. FUENTES NORMATIVAS Y JURISPRUDENCIALES

FUENTES NORMATIVAS

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal.

Decisión Marco 2005/222/JAI, del Consejo de 24 de febrero, relativa a los ataques contra los sistemas de información.

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

FUENTES JURISPRUDENCIALES

1991

Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, Sentencia de 28 de octubre de 1991- LA LEY 550/1992

1998

Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, 871/1998, de 19 de junio de 1998.

2002

Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, 994/2002, de 29 de noviembre (Rec. 1621/2001)

Sentencia del Tribunal Supremo núm. 1994/2002, Sala de lo Penal, de 29 noviembre. Recurso de Casación núm. 1621/2001. RJ 2002\10874

2005

Acuerdo del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo, reunión de 3 de febrero de 2005.

2010

Sentencia del Tribunal Constitucional núm. 37/2010 de 19 de julio

OTRAS RESOLUCIONES JUDICIALES

2011

SAP de Sevilla, Sección 7ª, de 30 de diciembre de 2011, Rec. 6474/2010.

2016

SAN, Sala de lo Penal, de 3 de marzo de 2016, Rec. 2/2016.