REVISTA DE DERECHO PENAL Y CRIMINOLOGÍA, 3.ª Época, n.º 25 (enero de 2021), págs. 77-124

SABOTAJE INFORMÁTICO A INFRAESTRUCTURAS CRÍTICAS: ANÁLISIS DE LA REALIDAD CRIMINAL RECOGIDA EN LOS ARTÍCULOS 264 Y 264 BIS DEL CÓDIGO PENAL. ESPECIAL REFERENCIA A SU COMISIÓN CON FINALIDAD TERRORISTA

María Concepción Gorjón Barranco

Universidad de Salamanca

Title: *Cybersabotage to critical infrastructures: analysis of the criminal reality set out in Articles 264 and 264 bis of the Criminal Code. Special reference to its commission for terrorist purposes*

Resumen: Los datos existentes sobre ciberataques con malware destructivo, botnets y denegación de servicios reflejan que estamos ante una nueva realidad criminal. Por eso, urge proteger los datos y sistemas informáticos, máxime cuando estos soportan servicios básicos para la ciudadanía como la energía, el agua, la salud, etc. Lograr este objetivo implica apostar en ciberseguridad y adoptar medidas en el ámbito legislativo. Por eso, nuestro legislador, entre otros ciberdelitos, tipificó en 2010 el sabotaje informático. Sin embargo, sin dudar de su necesidad, el reto desde la perspectiva penal, está en identificar la gravedad de esos ciberataques. Tomando en cuenta el criterio de la gravedad, haremos especial referencia en este trabajo, a aquellos que se dirigen a las infraestructuras críticas de los estados, recogido como una circunstancia agravante desde el año 2015 en los artículos 264 y 264 bis CP, así como a su comisión con finalidad terrorista del art. 573.2 CP.

Palabras clave: sabotaje informático; infraestructuras críticas; ciberseguridad; ciberterrorismo.

Abstract: *Cybercrime statistics about destructive malware, botnets and denial of services attacks, show that we are facing a new criminal reality. Therefore, it is necessary to protect data and computer systems which support basic services for citizens such as energy, water, health, etc. For this*

reason, States are investing in cybersecurity and taking legislative action. In Spain, cyber sabotage has been recognised as a crime since 2010. However, the challenge from the criminal law perspective is to identify the seriousness of these kinds of cyberattacks to consider them as crimes. By taking into account the severity of these crimes, in this paper, we will make special reference to those that target critical infrastructures, which is an aggravating circumstance in articles 264 and 264 bis of criminal code, and in addition to those that are committed for terrorist purposes under art. 573.2 CP.

Keywords: *cybersabotage; critical infrastructure; cybersecurity; cyberterrorism.*

1. Introducción

Los hospitales están librando una batalla fundamental durante la pandemia generada por el virus de la Covid-19. Durante el mes de marzo de 2020 en plena primera ola en España, el personal sanitario habría recibido correos electrónicos masivos que parecían contener información sobre el virus que, en realidad, encubrían un ciberataque. Esos correos portaban un ramsonware con el nombre de Netwalker cuya intención, según el Director Adjunto Operativo de la Policía, era "romper" el sistema informático de los hospitales[1]. Este hecho constituye un ejemplo que pone de manifiesto que ya estamos viviendo situaciones que hasta hace poco tiempo parecían propias de la ciencia ficción. Debemos evitar que esta crisis sanitaria represente una oportunidad para los ciberdelincuentes. Y lo cierto es que este no es un hecho aislado, sino que son ya muchos los casos conocidos que apuntan a que diversos ciberataques no solo provenientes de la criminalidad organizada o del ciberterrorismo,

[1] Según palabras del Director Adjunto Operativo (DAO) de la Policía Nacional en rueda de prensa Consultar en El País de 23 de marzo 2020, https://elpais.com/espana/2020-03-23/la-policia-detecta-un-ataque-masivo-al-sistema-informatico-de-los-hospitales.html (ultimo acceso: 31 de enero 2021).

sino también de otros países se están librando en el ciberespacio. Por eso, tampoco nos sorprende que existan comandos específicos de los distintos estados que operan en el ciberespacio para dañar infraestructuras críticas de otros países. Un ejemplo reciente que demuestra lo anterior, es el incidente protagonizado por Trump en junio de 2019, cuando el comando cibernético del Ejército de Estados Unidos lanzó un ataque digital contra el sistema informático militar de Irán[2]. En este punto, Llorec Valverde afirma que la ciberguerra se caracteriza por la utilización de "las tecnologías digitales para atacar y destruir sistemas estratégicos esenciales para nuestra forma de vida, empezando, por ejemplo, por los grandes centros de producción de energía eléctrica"[3].

En verdad, los países no solo están ampliando su capacidad ofensiva en el ciberespacio, sino también están apostando en ciberseguridad, esto es, en su capacidad para prevenir y repeler estos ataques de los distintos agentes que actúan en internet. Según lo dispuesto por la Unión internacional de telecomunicaciones (UIT[4]), una de las medidas para medir el compromiso de los países con la ciberseguridad es la implementación de medidas jurídicas[5]. En el caso de España, se han producido importantes cambios en nuestro código penal, de forma que en 2010 se introdujeron dos delitos específicos; los (mal denominados) delitos de daños a un sistema informático y los delitos de daños a los datos en él contenidos. Delitos que fueron objeto de modificación en 2015 resaltando como principal novedad, la inclusión de una agravante cuando el objetivo del ataque lo constituye un sistema que soporta una infraestructura crítica del Estado. Es por eso que lo que nos proponemos en este trabajo es analizar la realidad criminal que ha llevado a tipificar los delitos recogidos en los arts. 264 CP y 264 bis CP, con especial mención al sabotaje dirigido al sistema informático de una infraestructura crítica**,** así como el estudio de la elevación en 2015 de estos delitos a la categoría de ciberterrorismo en el art. 573. 2 CP. Este precepto considera terrorismo "los delitos informáticos tipificados en los artículos … 264 a 264 *quater* (entre otros) cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior", es decir, cuando el sabotaje, bien al sistema o bien a los datos contenidos en el sistema se lleven a cabo con la intención de: "1.ª Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a

[2] "EEUU lanzó un ciberataque a Irán este jueves autorizado por Trump". Consultar en El País de 24 de junio de 2020 https://elpais.com/internacional/2019/06/23/estados_unidos/1561302401_346950.html (último acceso: 31 de enero de 2021).

[3] Valverde, L., "Estamos perdiendo la ciberguerra: Estados Unidos lleva tiempo usando la tecnología digital para atacar a sus enemigos", en EL País de 16 de Julio de 2013. Consultar en El País http://elpais.com/elpais/2013/07/12/opinion/1373622319_413845.html (último acceso: 31 de enero de 2021).

[4] Organismo de las Naciones Unidas para las tecnologías de la información y comunicación.

[5] Índice Mundial de ciberseguridad y perfiles de *ciberbienestar (IMC)*, UIT, 2015, p. 1.

los poderes públicos a realizar un acto o a abstenerse de hacerlo. 2.ª Alterar gravemente la paz pública. 3.ª Desestabilizar gravemente el funcionamiento de una organización internacional. 4.ª Provocar un estado de terror en la población o en una parte de ella." Es por ello, que el último apartado de este trabajo lo dedicaremos a su estudio. Trataremos de delimitar estos tipos penales para ajustarlos no solo a la literalidad de los instrumentos internacionales existentes, sino a la realidad que estos instrumentos parecen referir, así como a la gravedad de los ataques en cada caso concreto.

2. Conceptos

2.1. Sabotaje a sistemas informáticos o a los datos en él contenidos

La Estrategia de ciberseguridad nacional de 2013 no da una definición concreta de ciberataque, pero sí apunta ciertas características que hacen de ellos el medio perfecto para crear el caos en internet. En primer lugar, se destacaba su bajo coste, pues las herramientas necesarias pueden adquirirse gratuitamente o a un precio muy reducido. En segundo lugar, su ubicuidad y fácil ejecución, porque no se precisan grandes conocimientos técnicos y su ejecución no depende de la localización de los ciberdelincuentes. En tercer lugar, su efectividad e impacto, porque si el ataque está bien diseñado, es fácil que logre los objetivos que pretende. Finalmente, se destaca el reducido riesgo para el atacante porque puede ocultarse fácilmente, complicando la atribución de la comisión de un ciberataque a su verdadero autor o autores, unido a un marco legal dispar o inexistente que dificulta la persecución de la acción[6]. Más específicamente a los fines de nuestro trabajo, la literatura especializada destaca tres elementos en los ciberataques más graves; el primero es que no persigue una ventaja económica. El segundo, que tampoco se realiza con el propósito de obtener información (ciberespionaje), y el tercero y más importante es, que interrumpe o destruye una red computarizada y puede llevar a la interrupción de los equipos conectados en la red bajo ataque[7]. Esta definición es acorde al diccionario del Departamento de defensa de EEUU, que la describe como aquella acción llevada a cabo en el ciberespacio que crea efectos notables de negación, es decir, de degradación, interrupción o destrucción[8]. Por todo ello, también resulta

[6] Estrategia de ciberseguridad nacional 2013, Capítulo I: "El ciberespacio y su seguridad". Consultar en https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ES_NCSS.pdf (último acceso: 31 enero de 2021).

[7] Ambos, K., "Responsabilidad penal internacional en el ciberespacio", *Indret: Revista para el análisis del Derecho*, núm. 2, 2015, p. 3.

[8] Departamento de Defensa de EEUU, *DOD Dictionary of Military and Associated Terms*, June 2020. Define "Cyberspace attacks", como: *"actions taken in cyberspace that*

interesante la distinción que realiza Romeo Casabona cuando atiende la finalidad de esos ataques, estableciendo que algunos sabotajes se dirigen a causar un perjuicio patrimonial y otros llevan aparejada una finalidad política. Nos interesan sobre todo estos últimos, donde el objetivo es la desestabilización logística y organizativa del aparato del Estado, que se antepone al de causación de un perjuicio económico[9], máxime añadimos nosotros, cuando alcanzan una infraestructura crítica de un país. Nos centraremos en el segundo tipo de incidentes por ser más acordes a la finalidad perseguida en este trabajo.

Concretando un poco más, el término sabotaje informático alude a dos tipos de incidentes. Por un lado, aquellos que se ejecutan sobre datos o programas de un sistema informático[10] y, por otro los que se dirigen contra el propio sistema[11]; ya sea mediante el envío de virus, o por cualquier otra forma de destrucción o inutilización, bien de archivos o datos de terminales concretos. De tal forma que puede afectar al hardware, esto es, a los propios sistemas informáticos, o al software, es decir, a la información, bien sea de los datos o de los programas informáticos contenidos en los sistemas[12]. Aunque las conductas de uno y otro delito son similares, podemos adelantar que la diferencia esencial "vendría determinada por la capacidad de la acción para afectar a la operatividad o al funcionamiento del sistema informático en su conjunto"[13].

La forma más popular de sabotaje informático es aquella que se lleva a cabo mediante distribución de software malicioso denominado malware, destinado a dañar, controlar o modificar un sistema informático[14]. No todos los malware tienen la misma capacidad destructiva, sino que

---

create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires". En https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (Último acceso: el 31 de enero de 2021).

[9] Romeo Casabona, C. M., "Los delitos de daños en el ámbito informático", en *Cuadernos de Política criminal. Núm. 43*, 1991, p. 92.

[10] Creemos que el término sabotaje de datos informáticos y de sistemas informáticos es mejor que el de daños a datos informáticos o sistemas informáticos, siguiendo a Robles Planas, R. y Pastor Muñoz, N., "Tema 12: Delitos contra el patrimonio (III)", en VVAA, *Lecciones de Derecho Penal, Parte especial, Cuarta edición adaptada a la LO 1/2015 de reforma del CP*, Atelier, Barcelona, 2015, p. 294.

[11] De otra parte, utilizando indistintamente el término sabotaje o daños informáticos Morón Lerma, E., "Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos", en *Cuadernos penales José María Lidón: Delito e informática: algunos aspectos*, núm. 4, Universidad de Deusto, Bilbao, 2007, p. 108.

[12] Miró Llinares, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* Marcial Pons, Madrid, 2012, p. 58.

[13] Circular 3/2017 de la FGE de 21 de septiembre, sobre la reforma del código penal operada por LO 1/2015, de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos, p. 37. Consultar en https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2017-00003.pdf (Último acceso: 31 de enero de 2021).

[14] Miró Llinares, *op. cit*., pp. 57-58.

responden a diferentes funciones. Por ejemplo, los virus y los gusanos se caracterizan por infectar sistemas. Los rootkits, troyanos y puertas traseras (o backdoors) son tipos de malware que se utilizan para ocultar otros malware. Por su parte, los keyloggers capturan pulsaciones de teclas y los stealers se utilizan para el robo de información privada. Los spyware, adware y hijacking realizan diferentes funciones como mostrar anuncios no solicitados, recopilar información privada o redirigir solicitudes de páginas, etc[15]. Sí que podría crear efectos más graves el ransomware, que cifra ficheros, y bloquea dispositivos[16] también conocido como criptovirus o secuestrador, por su capacidad de cifrar todos o parte de los archivos del sistema dejándolos inaccesibles al legítimo usuario[17]. Por su parte, las bombas lógicas son rutinas introducidas en un programa para que, al ejecutar una determinada acción, se produzcan alteraciones o daños en el programa[18]. También las botnets, que permiten el acceso remoto. En concreto una botnet es capaz de controlar muchos ordenadores de usuarios de forma remota para propagar virus, generar spam y cometer otros tipos de delitos y fraudes en la Red. Esto quiere decir, según la Oficina de Seguridad del Internauta que, alguien sin estar físicamente delante de un ordenador, pero con los conocimientos técnicos suficientes puede manejarlo a su antojo. Pero eso no es todo, si ese ordenador es un zombi, estará formando parte de una red zombi de ordenadores, más conocido por el término anglosajón botnet, que no es más que un gran número de ordenadores zombi infectados con el mismo tipo de virus que están controlados por una misma persona u organización criminal (botmaster)[19].

Otra forma de sabotaje con capacidad destructiva, sería un ataque de denegación de servicios (DOS), que, atendiendo a lo dispuesto en un estudio sobre seguridad realizado por Soriano, incluiría todo tipo de ataques destinados a saturar un ordenador o a una red, de tal manera que los usuarios legítimos no pueden utilizarla[20]. Una versión mejorada de los ataques DOS, son los ataques distribuidos de denegación de servicios (ataques DDOS), que se produce cuando varias máquinas, de manera

---

[15] Gil Gil, A. y Hernández Berlinches, R. (Coords.), *Cibercriminalidad*, Dykinson, Madrid, 2019, pp. 61-66.

[16] Oficina de Seguridad del Internauta: https://www.osi.es/es/actualidad/blog/2016/05/31/el-ransomware-cada-vez-mas-peligroso-protegete (Último acceso: 31 enero de 2021).

[17] Gil Gil y Hernández Berlinches (coords.), *op. cit.*, p. 67.

[18] De La Mata Barranco, N. J. y Hernández Díaz, L., "El delito de daños informáticos: una tipificación defectuosa", en *Revista de Estudios penales y criminológicos*, vol. XXIX, 2009, p. 315.

[19] Oficina de Seguridad del Internauta: https://www.osi.es/es/actualidad/blog/2014/03/14/que-es-una-botnet-o-una-red-zombi-de-ordenadores (Último acceso 31 de enero de 2021).

[20] Soriano, M., "Seguridad en redes y seguridad de la información", *Improvet: Proyecto financiado por la Comisión Europea*, Publicado por České vysoké učení technické v Praze, p. 11. Consultar en https://docplayer.es/4814747-Seguridad-en-redes-y-seguridad-de-la-informacion-miguel-soriano.html (Último acceso 31 de enero de 2021).

coordinada atacan a una sola víctima, complicando las estrategias defensivas del servidor o sistema atacado[21]. En cualquier caso, tanto los ataques DOS como los DDOS suponen una coacción doble, porque, de un lado, impiden al titular de la página comunicar el contenido, con las consecuencias económicas que pueda conllevar, cuando se trata por ejemplo de páginas de venta directa de productos, o las consecuencias para la libertad de expresión, cuando el ataque consista en hacktivismo político. Y, por otro lado, también impiden al usuario acceder a la comunicación[22].

Estos ciberataques cobran especial relevancia en casos graves cuando, por ejemplo, interrumpen o destruyen los sistemas que soportan infraestructuras críticas de los Estados, afectando derechos básicos de los ciudadanos y no tanto cuando se trata de alcanzar datos o sistemas particulares. Una circunstancia que en nuestro código penal se recoge a partir de la reforma de 2015 como agravante y, que aquí, pretendemos reivindicarlo como un elemento esencial a tener en cuenta.

2.2. Identificación y protección de infraestructuras críticas: una aproximación europea y nacional

Nuestras sociedades dependen cada vez más de un complejo sistema de infraestructuras que soportan los sectores productivos, de gestión y de desarrollo de la vida ciudadana en general. Unas infraestructuras que son interdependientes entre sí, motivo por el que pueden desencadenar problemas de seguridad en cascada a través del propio sistema, con la posibilidad de ocasionar fallos inesperados y graves en servicios básicos para la población[23]. Se engloban aquí aquellos sistemas informáticos que soportan infraestructuras que proporcionan los servicios esenciales a la sociedad, como salud, energía, industria, etc., cuyo ataque podría suponer una situación crítica para el bienestar de los ciudadanos.

Este tipo de infraestructuras son especialmente atractivas para el terrorismo, por los graves daños que pueden ocasionarse para la población. Por eso, no es casual que, en el seno de la Unión europea, el 20 de octubre de 2004 la Comisión adoptara una Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo que contenía propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas[24]. También, en diciembre de 2004, el Consejo aprobó el Programa europeo de protección de infraestructuras

[21] Miró Llinares, *op. cit*., p. 64.

[22] *Ibidem* , p. 65.

[23] Exposición de motivos de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

[24] Comunicación de la Comisión al Consejo y al Parlamento Europeo: Protección de las infraestructuras críticas en la lucha contra el terrorismo / COM / 2004/0702 final /.

críticas (PEPIC) y puso en marcha una red de información sobre alertas en infraestructuras críticas (*Critical Infrastructures Warning Information Network*-CIWIN). De esta forma, daría comienzo un proceso de identificación y designación de las infraestructuras críticas europeas (las ICE) que desembocaría en la Directiva 2008/114, del Consejo, de 8 de diciembre, *sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección*. Según el art. 2 de esta Directiva, debe entenderse por infraestructura crítica: "el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones".

En referencia a cómo se ha desarrollado en España esta labor de identificación y protección, habría que atender en primer lugar al Plan Nacional de Protección de las Infraestructuras Críticas, de 7 de mayo de 2007, así como la elaboración de un primer Catálogo Nacional de Infraestructuras Estratégicas y la aprobación en el Consejo de Ministros de 2 de noviembre de 2007, de un Acuerdo sobre Protección de Infraestructuras Críticas. Resultado de lo anterior, se identifican dieciocho áreas que necesitan del desarrollo de un Plan Estratégico Sectorial (PES), que son: Energía (electricidad, gas y petróleo); Industria Nuclear; Sistema Financiero; Transporte (aéreo, carreteras, ferrocarril y marítimo); Agua; Espacio; Industria Química; TIC; Transporte Urbano y Metropolitano; Alimentación y Salud[25]. De esta forma, en el año 2007 se creó el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), que es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior[26].

Además, cumpliendo con la transposición de la Directiva europea de 2008, se aprobó en España la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Esta Ley en su preámbulo, insiste en la amenaza del terrorismo destacando que; los "nuevos riesgos, generados, en gran medida, por la globalización, y entre los que se cuentan el terrorismo internacional, la proliferación de armas de destrucción masiva o el crimen organizado, se suman a los ya existentes, de los cuales el terrorismo tradicional venía siendo un exponente". Así mismo, el Real Decreto 704/2011, de 20 de mayo, por

[25] Comisión Nacional para la protección de infraestructuras críticas, https://www.dsn.gob.es/es/actualidad/sala-prensa/comisi%C3%B3n-nacional-para-protecci%C3%B3n-infraestructuras-cr%C3%ADticas (Último acceso: 31 de enero de 2021).

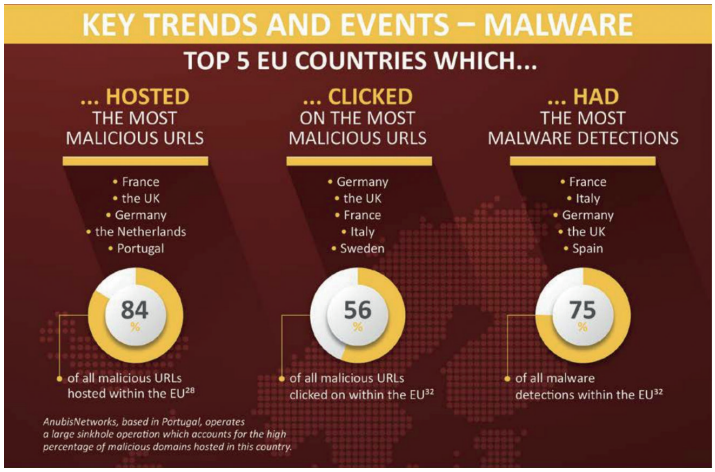
[26] Centro nacional para la protección de las infraestructuras críticas; http://www.cnpic.es/ (Último acceso: 22 de septiembre 2020).

el que se aprueba el Reglamento de protección de las infraestructuras críticas, insiste en el diseño de un planteamiento orientado a prevenir y proteger las denominadas infraestructuras críticas de las amenazas o actos intencionados provenientes de figuras delictivas como el terrorismo, potenciados a través de las tecnologías de la comunicación[27].

Por tanto, de la normativa europea y española, se deduce una especial consideración a la protección de estas infraestructuras frente a ataques terroristas, quizás por eso, el legislador español en 2015 decidió introducir en el código penal este fenómeno dentro del art. 573.2 CP, y que analizaremos al final del trabajo.

3. La realidad criminal que reflejan los datos

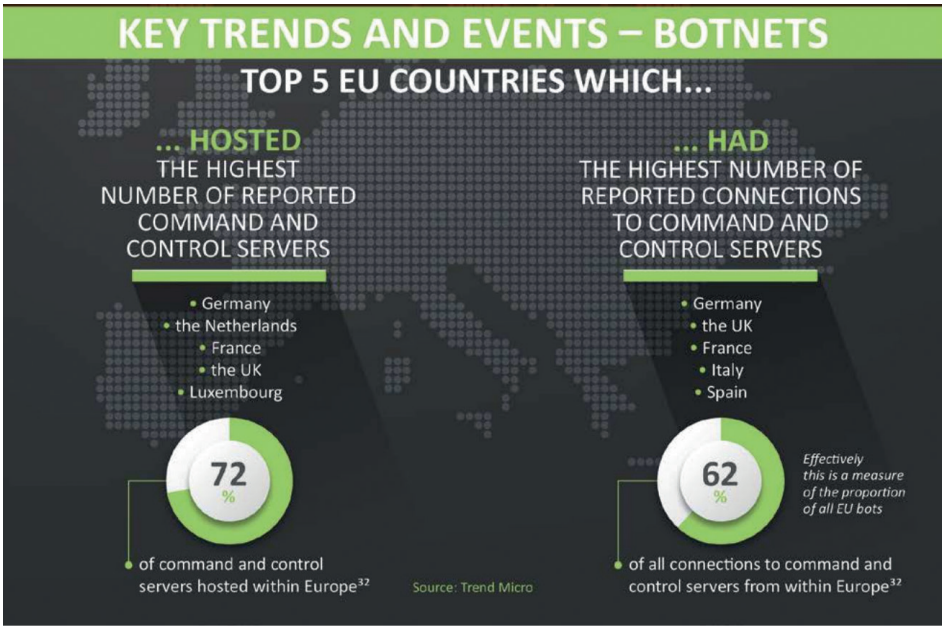
Según el informe de Europol: *Evaluación de Amenazas del Crimen organizado en internet* (IOCTA) de 2017, nuestro país destaca en el ranking en la posición número cinco de Europa con mayores detecciones de malware (cuadro 1) y botnets (Cuadro 2), como puede comprobarse en los cuadros siguientes[28].



Fuente: Europol. IOCTA, 2017

[27] Real Decreto de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, BOE núm. 121, de 21 de mayo de 2011.

[28] Informe: Evaluación de Amenazas del Crimen organizado en internet, Europol, 2017, p. 24.



Fuente: Europol. IOCTA, 2017

Siguiendo lo dispuesto en el mencionado Informe de Europol, IOCTA del año 2018 y, en referencia a ataques dirigidos a los sistemas que soportan las infraestructuras críticas de los estados, se afirma que, dentro de la Unión Europea estos ataques afectaron a una amplia gama de industrias clave e infraestructuras críticas, incluidos los servicios de salud, telecomunicaciones, transporte e industria manufacturera[29]. De la misma forma y en la línea de estos datos aportados por Europol, en España el Ministerio del Interior dentro de su Estudio sobre la cibercriminalidad en España (2017), advierte que el tipo de incidentes con mayor repercusión en los operadores críticos fue el código dañino (malware) y, desde el año anterior los ataques de denegación de servicios (DOS) habrían aumentado en un 96,43%[30]. Además, se observa que, durante 2017 el sector estratégico más atacado en España fue el sector financiero y tributario, seguido de los sectores de la energía, transporte y agua respectivamente[31].

[29] Informe: Evaluación de Amenazas del Crimen organizado en internet, Europol, 2018, p. 16.
[30] Estudio sobre la Cibercriminalidad en España, Ministerio del Interior, 2017, pp. 25-28.
[31] *Ibidem* , p. 28.

Sector estratégico	INCIDENTES GESTIONADOS			
	2014	2015	2016	2017
Energía	34	46	126	213
Transporte	14	24	90	152
Tegnologías Informac. y Comunicac. (TIC)	6	17	17	40
Sistema tributario y financiero	3	17	152	250
Alimentación	0	12	47	42
Agua	0	5	40	134
Industria nuclear	4	5	4	12
Administración	2	1	2	10
Espacio	0	0	0	1
Industria química	0	0	0	0
Instalaciones de Investigación	0	0	0	0
Salud	0	0	0	1
Todos los sectores afectados	0	3	1	0

Fuente: Ministerio del Interior: "Estudio sobre la Cibercriminalidad en España", 2017

Ante la evolución y el incremento de ciberataques a infraestructuras clave para la ciudadanía se demandan estrategias que desarrollen la capacidad de respuesta de los diferentes países. En este sentido, analizaremos las estrategias sobre ciberseguridad aprobadas en Europa y en España.

4. Ciberseguridad

4.1 Estrategias sobre ciberseguridad

Ante la amenaza que representan este tipo de ciberataques, no todos los países han adoptado las mismas medidas sobre ciberseguridad. Por eso, la Unión internacional de Telecomunicaciones (UIT), insiste en la necesidad de "fomentar la sensibilidad sobre la ciberseguridad y la importancia del papel que deben desempeñar los gobiernos en la integración de los mecanismos oportunos para apoyar y promover esta disciplina crucial. La salvaguardia de la integridad del ciberespacio debe conllevar el desarrollo de la ciberseguridad"[32]. Por eso, en su índice mundial de ciberseguridad y perfiles de ciberbienestar (IMC), mide el nivel de compromiso de los países con la ciberseguridad en cinco ámbitos; medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación internacional[33]. En su informe de 2015, establece un listado de países donde refleja el compromiso de cada uno de ellos con la ciberseguridad. Los países a la cabeza son Estados Unidos y Canadá en el primer y segundo puesto respectivamente[34]. España

[32] Índice Mundial de ciberseguridad y perfiles de *ciberbienestar (IMC*), UIT, 2015, p. 1
[33] *Ibidem* .
[34] *Ibidem* , consultar cuadro de las pp. 1 y 2.

ocuparía el puesto 9, empatada con países como Colombia, Dinamarca, Egipto, Francia y Mauricio[35].

Para identificar y prevenir estos ataques a nivel europeo, cabe resaltar la *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro de 2013*, centrada en cinco prioridades estratégicas: a) Lograr la ciberresiliencia. b) Reducir drásticamente la ciberdelincuencia. c) Desarrollar estrategias y capacidades de ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD). d) Desarrollar recursos industriales y tecnológicos de ciberseguridad. e) Establecer una política internacional coherente del ciberespacio para la Unión Europea y promover los valores esenciales de la UE[36]. A los fines de este trabajo, especial mención merece la estrategia relativa a reducir la ciberdelincuencia (la prioridad b), en cuyo desarrollo se especifica la necesidad de una normativa estricta y eficaz en referencia a la adopción por parte de los Estados de lo dispuesto en el Convenio sobre la ciberdelincuencia de 2001 (más conocido como Convenio de Budapest) y en las Directivas europeas que lo desarrollan, instrumentos que serán objeto de análisis más adelante en este trabajo.

Siguiendo con el desarrollo de la ciberseguridad en Europa, debemos resaltar también la Directiva 2016/1148/UE del Parlamento Europeo y del Consejo, *relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión,* conocida como Directiva NIS, centrada especialmente en reforzar la detección y prevención de ataques informáticos. Esta Directiva define la seguridad de las redes y sistemas de información como "la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos". Entre otras cuestiones, "introdujo obligaciones relativas a medidas de seguridad y notificaciones de incidentes en todos los sectores fundamentales de la economía y la sociedad, como la energía, los transportes, el agua potable, el suministro y la distribución, la banca, las infraestructuras de los mercados financieros, la sanidad o las infraestructuras digitales, así como para los proveedores de servicios digitales clave (motores de búsqueda, servicios en la nube y mercados en línea)"[37]. Resaltamos esa necesidad de

[35] *Ibidem* , consultar cuadro de la p. 6.

[36] Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro en 2013, Bruselas, 7.2.2013, JOIN (2013) 1 final.

[37] Reglamento (UE) 2019/881 del Parlamento europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por

notificar los casos, en aras a conocer tanto la dimensión del fenómeno, como la procedencia de los riesgos, para de ese modo, poder prevenirlos y castigarlos.

Por último, en el seno de la UE se ha aprobado el Reglamento (UE) 2019/881 del Parlamento europeo y del Consejo de 17 de abril de 2019 *relativo a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación*, y por el que se deroga el Reglamento (UE) no 526/2013 (Reglamento sobre la Ciberseguridad)[38]. Este nuevo Reglamento define ciberseguridad como "todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas".

A nivel nacional, fue en 2013 cuando se aprobó la primera Estrategia nacional sobre ciberseguridad, cuya finalidad era "implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas"[39]. La Estrategia gira en torno a un objetivo global que es "lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques". Este objetivo general se concreta en otros específicos, como el dedicado a "impulsar la seguridad y resiliencia de los Sistemas de Información y Telecomunicaciones usados por los operadores de infraestructuras críticas" (objetivo II), o el de "potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio" (objetivo III)[40]. Una vez más hace aparición la preocupación por el terrorismo internacional.

Por su parte, la segunda Estrategia sobre ciberseguridad nacional de 2019, examina en su segundo capítulo las principales amenazas y desafíos del ciberespacio a los que se enfrenta España. Se pone de manifiesto que, tanto "actores estatales y no estatales, bien de forma directa o a través de intermediarios, explotan las facilidades que ofrece Internet y que existe un interés generalizado en el desarrollo de capacidades militares para operar en el ciberespacio, que en muchos casos incluyen capacidades ofensivas"[41]. Se menciona de nuevo, específicamente, la actividad de

---

el que se deroga el Reglamento (UE) n. 526/2013 («Reglamento sobre la Ciberseguridad»), en su considerando 15.

[38] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

[39] Estrategia de ciberseguridad nacional 2013 en su Resumen ejecutivo.

[40] *Ibidem* . Los objetivos se plasman en el Capítulo III: "Objetivos de la ciberseguridad".

[41] Estrategia Nacional de Ciberseguridad 2019, en su capítulo II dedicado a "Las amenazas y desafíos en el ciberespacio". Consultar en https://www.boe.es/eli/es/o/2019/04/26/pci487 (Último acceso: 31 de enero de 2021).

los grupos terroristas, quienes "tratan de aprovechar las vulnerabilidades del ciberespacio para realizar ciberataques …. Íntimamente relacionado con ello, se halla la amenaza contra las infraestructuras críticas, con la posibilidad cierta de causar un colapso a través de las redes mediante una caída en cadena de los servicios esenciales"[42]. Su capítulo III está dedicado a los objetivos para la ciberseguridad, definiendo de nuevo como uno de los objetivos (el II) la necesidad de un *uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso*[43]. En este punto la estrategia resalta la necesidad de una regulación sólida y eficaz que refuerce y garantice la lucha contra la cibercriminalidad.

4.2. Contexto actual: procedencia de los riesgos. Especial referencia al ciberterrorismo

En una entrevista de 2018, Steve Purser, director de la Agencia Europea de Seguridad de las Redes y de la información (ENISA), advertía del riesgo de un posible ataque a las infraestructuras críticas de los países europeos, sin concretar si éstos podrían venir patrocinados por otros Estados, indicando las altas posibilidades de procedencia terrorista[44]. Lo cierto es que, tanto las estrategias sobre protección de infraestructuras críticas, como las estrategias sobre ciberseguridad analizadas hasta ahora, se centran sobre todo en la ciberamenaza que representan las actividades terroristas.

Pues bien, tomando de referencia estos hechos más graves, y según los datos obrantes en el Informe sobre la situación y las tendencias del terrorismo de Europol, se observaba en 2016, que los terroristas se estarían beneficiando del modelo CaaS (crimen como servicio), proporcionándoles las herramientas, servicios y vectores de ataque necesarios. El informe preveía como un posible escenario un ataque de denegación de servicio distribuido (DDoS) con el objetivo de interrumpir infraestructuras críticas. Además, los terroristas al poder operar desde lugares remotos estarían minimizando el riesgo de detección, que sí se crearía al viajar o preparar un ataque en el país de destino. Por lo tanto, se prevé la probabilidad de que futuros ataques se basen en un nuevo *modus operandi* con una dimensión cibernética más sólida, porque los terroristas están demostrado flexibilidad y voluntad de aprender y desarrollar a sus

[42] *Ibidem* .
[43] *Ibidem* , Capítulo III: "Propósito, principios y objetivos para la ciberseguridad".
[44] Steve Purser es el Director de operaciones de ENISA; "Europa debe temer ataques a infraestructuras críticas. El director de Operaciones de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) advierte de los riesgos y los avances en protección informática", en El País, a 11 de mayo de 2018. Consultar en https://elpais.com/tecnologia/2018/05/08/actualidad/1525777307_994204.html (ultimo acceso:31 de enero de 2021).

habilidades técnicas[45]. Sin embargo, esta descripción de Europol parece referir todavía una amenaza de ciberataque, un posible escenario más que una realidad.

En este punto, nos parece importante reivindicar un concepto restringido de ciberterrorismo, solo para los casos donde los sistemas sean el propio objeto de ataque y no solo el medio por el que discurre el delito. Sin embargo, está muy admitido su utilización extensiva, ampliando el concepto a cualquier uso que hagan los terroristas de las TIC para la propaganda terrorista, por ejemplo. Por eso, estamos de acuerdo con Ortigosa, en apostar por una concepción estricta de ciberterrorismo, reservando el término para los casos que impliquen "la realización de acciones ofensivas contra los sistemas de información y comunicación que sustentan el normal funcionamiento de las denominadas infraestructuras críticas y estratégicas, así como cualquier otro servicio esencial para la ciudadanía"[46].

Por su parte, el informe sobre Ciberamenazas y tendencias de 2017 del Centro Criptológico Nacional, parece reconocer que el mayor peligro es el ataque con origen en estados extranjeros[47]. Este dato nos resulta muy interesante. Como ocurrió en el caso de los ciberataques a compañías de electricidad de Ucrania que, en 2016 ocasionaron un apagón, provocando que entre 700.000 y 1,4 millones de personas se quedaran sin energía eléctrica[48]. En referencia a lo ocurrido en territorio español, el referido informe esquematiza los agentes de las amenazas más significativas atendiendo tanto a la tipología de sus acciones como a sus víctimas. De toda la información ofrecida, destacan aquellas acciones que tienen una finalidad política, corroborando que los Estados tienen una capacidad ofensiva más o menos desarrollada y, entendiendo por el contrario que ciberterroristas y ciberyihadistas todavía no tienen como objetivos ni a los Estados ni a las organizaciones privadas, utilizando simplemente el ciberespacio con fines de propaganda y reclutamiento y, cuyas principales víctimas son las organizaciones privadas y los ciudadanos[49]. Otro dato sin duda muy interesante. Podemos deducir, que más allá de los riesgos de posibles amenazas, los datos reconocen que la amenaza de ciberataques graves tiene su origen en otros estados, y no tanto en las organizaciones terroristas internacionales.

---

[45] Informe sobre la situación y las tendencias del terrorismo en la UE (TE-SAT), Europol, 2016, p. 8.

[46] Ortigosa, A., "Las nuevas amenazas cibernéticas del s. XXI. Ciberterrosrimo: nueva forma de subversión y desestabilización", en *Cuadernos de la Guardia Civil. Revista de Seguridad pública*, 3ª época, 2016, p. 109.

[47] Informe: *Ciberamenazas y tendencias*, 2017, del Centro Criptológico Nacional, CCN-CERT IA-16/17, p. 12.

[48] *Ibidem* , p. 8.

[49] *Ibidem* , p. 11.

Respecto de la estrategia de lucha contra estos ciberataques, ciertamente debemos partir de la idea de legitimidad del uso de la violencia por parte del Estado, y, por el contrario, de la falta de la misma en los terroristas, lo que lleva necesariamente a valorar que las acciones de unos y otros se ubican en planos morales y tácticos diferenciados[50]. Pero ese derecho de los estados también implica obligaciones traducidas en límites que les impide extralimitarse en sus funciones. Por tanto, cabría preguntarse si es legítimo que, tal y como se desprende del informe antes citado, un estado use herramientas desde el ciberespacio para alcanzar objetivos tácticos o estratégicos de otros estados y en qué circunstancias deben utilizarse estos recursos.

Pese a los datos que acabamos de analizar, que parecen indicar que el desarrollo de capacidades ofensivas es mayor en los estados que en los terroristas, las respuestas se han centrado en el ciberterrorismo, quizás, porque, pese a la existencia de la ciberguerra entre Estados, como afirmara el secretario general de la ONU, Antonio Guterres, no está clara cuál debe ser su respuesta, si se debería recurrir a la Convención de Ginebra o al Derecho internacional[51]. Aunque existiera un consenso internacional en aplicar el Derecho internacional también en el ciberespacio[52], el problema es que los actores-Estado con Gobiernos totalitarios mantienen ciertas ventajas a la hora de llevar a cabo este tipo de ataques sin control alguno, ya que esos ataques no están limitados por una supervisión estatal o la transparencia[53].

5. Agentes en internet con finalidad política: casos destacados

5.1. Estados

La ciberguerra tendría por protagonistas a los Estados que atacan páginas web de otros gobiernos, obstruyendo así la vida política de los mismos[54]. Aunque los miedos sociales y el código penal se centran en la

[50] Alonso, R.; "El terrorismo islamista inspirado en el Islamismo radical", en *Cuadernos de la Guardia Civil, Revista de Seguridad pública*, 3ª época, 2016, p. 87.

[51] Puede consultarse en: "El Secretario general de la ONU dice que hay ciberguerra entre Estados. Antonio Guterres defiende crear una regulación internacional para evitar riesgos que son reales", en *El País* de 19 de febrero de 2018, consultar en https://elpais.com/internacional/2018/02/19/actualidad/1519058033_483850.html. (Último acceso 16 de septiembre de 2020).

[52] Sobre esta problemática, consultar Pérez-Prat Durbán, L., "Los ciberataques y el uso de la fuerza en las relaciones internacionales", en Millán Moro, L. (dir.), *Ciberataques y ciberseguridad en la escena internacional,* Aranzadi, Pamplona, 2019, p. 17.

[53] Villalba Fernández, A. y Corchado Rodríguez, J. M., "Análisis de las ciberamenazas", en *Cuadernos de estrategia*, núm. 185, 2017, p. 112.

[54] Miró Llinares, *op. cit*., p. 134.

amenaza terrorista, lo cierto es que existen evidencias de que determinados países disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la Seguridad Nacional de otros estados[55]. Valverde, afirma que la tercera Guerra Mundial tiene como escenario el ciberespacio, que ya se ha convertido en un nuevo campo de batalla militar[56]. Afirma este autor que es de todos conocido que, el primero en usar las tecnologías digitales como herramienta de sabotaje fue Estados Unidos, en los años ochenta, contra la economía soviética. Conocido como el caso Farewell donde los americanos fueron capaces de colocar chips destinados a controlar los sistemas de un gasoducto ruso, provocando una de las mayores explosiones no termonucleares de la historia[57].

A éste primer episodio le han sucedido otros muchos casos, como el ataque, esta vez de Rusia contra Estonia en 2007 por la retirada de la estatua del soldado soviético de un parque de Tallín. Los ciberataques llegaron a inutilizar y colapsar el ciberespacio de Estonia durante un mes. También Rusia en el verano de 2008 atacó a Georgia a raíz del conflicto del Caúcaso por el control del enclave estratégico de Osetia del Sur, llevando a una serie de ataques de denegación de servicios (DDOS) que precedieron a una incursión militar sobre el territorio de Georgia. Para la mayoría de los analistas se trató de un caso clave de ciberguerra hablando de hackers patrióticos o cibermilicianos[58]. Al igual que en 2010 Israel infectó con el virus Stuxnet a los sistemas informáticos del programa nuclear iraní[59].

En los últimos años cabe resaltar el ciberataque conocido como *Not-Petya* que arrancó en Ucrania en 2017 y se extendió después por Europa, EEUU y la India afectando principalmente al sector financiero y al energético. Se acusó a Moscú del ataque como parte de la guerra híbrida que enfrentaba a ucranianos y rusos desde la anexión de Crimea[60]. Ciertamente, los efectos reales "fueron de escasa entidad, pero sirvieron para poner de manifiesto su potencialidad y capacidad de difusión, el riesgo efectivo que entrañan y las graves consecuencias que pueden tener en el normal funcionamiento de organismos e instituciones de todo tipo e incluso en el desenvolvimiento de las relaciones políticas, sociales y/o económicas nacionales e internacionales"[61].

---

[55] *Estrategia de ciberseguridad nacional 2013*, p. 10.
[56] Valverde, *op. cit.*
[57] *Ibidem*.
[58] Ortigosa, *op. cit.*, p. 112.
[59] Para más información sobre estos casos Miró Llinares, *op. cit.*, pp. 133-134.
[60] Pérez-Prat Durbán, *op. cit.*, p. 30.
[61] Memoria de la Fiscalía General del Estado (FGE) 2018, Capítulo III. Apartado 8: Criminalidad informática. Consultar en https://www.fiscal.es/memorias/memoria2018/FISCALIA_SITE/index.html (Último acceso: 22 de septiembre de 2020).

5.2. Ciberterrorismo y acciones afines

El objetivo de los grupos terroristas es provocar cambios políticos a través de acciones que provoquen pánico y terror en las sociedades, pero su actividad grave en internet parece todavía un escenario del futuro, una amenaza[62]. Si bien, la irrupción de las TIC y su impacto en el nuevo terrorismo ha llevado a hablar de una UHMA digital[63]. La red de redes se ha convertido sobre todo en un instrumento para la captación y radicalización, así como en un medio de propaganda de sus actos y no tanto en objetivo de sus acciones, que sigue siendo más una posibilidad que una realidad, ya que los caminos de los hackers y los terroristas parece que no han confluido[64]. De forma que hasta ahora, los ataques más conocidos que se han dado por parte del terrorismo internacional a sistemas de información son los siguientes:

En 2015 la cadena francesa de televisión TV5 Monde sufrió un ciberataque a mando del autodenominado CiberCalifato vinculado a Daesh, que bloqueó la emisión de la señal de la televisión satélite de esta cadena, así como su web y redes sociales[65]. También se tienen evidencias de que los "terroristas han manipulado páginas electrónicas de empresas privadas u organismos internacionales para crear en ellas ficheros adjuntos con propaganda. Es el caso del video del rehén Paul Johnson que apareció en primicia mundial en la página electrónica de la empresa Sillicon Valley Land Surveying con sede en San José (California), lo que constituyó una auténtica revolución mundial en las técnicas de propaganda y una emulación de las formas de trabajo empleadas casi exclusivamente hasta ese momento por cibercriminales o piratas informáticos"[66].

Del mismo modo cabe resaltar los ataques a la cuenta de Twitter del cantante Justin Bieber en febrero de 2016, publicando un video titulado: "Un mensaje al Islam de occidente" cuyo contenido consistía en un llamamiento a los fieles de unión a la causa islámica, y en la que se veía la ejecución de cuatro hombres. Además, utilizaron el hashtag #JustinBieber para mandar mensajes como respuesta a que el cantante condenara lo ocurrido en la sala Bataclán de conciertos de París[67]. En este mismo ámbito se puede atribuir al ciberejército yihadista, el diseño de la aplicación móvil *Dawn of Glad Tidings* que enlaza con tuits a través de sus

---

[62] Villalba Fernández y Corchado Rodríguez, *op. cit.*, p. 113.

[63] González Cussac, J.L., "Servicios de inteligencia y contraterrorismo", en Portilla Contreras, G. y Pérez Cepeda, A. (dirs.), *Terrorismo y contraterrorismo en el s. XXI. Un análisis penal y político criminal*, Ratio Legis, Salamanca, 2016, pp. 121-122.

[64] Ruíz Díaz, J., "Ciberamenazas, ¿el terrorismo del futuro?", en *Boletín IEEE*, núm. 3, Julio-septiembre, 2016, p. 541.

[65] Ortigosa, *op. cit.*, p. 113.

[66] Merlos García, A.; "Internet como instrumento para la Yihad", en *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades*, núm. 16, diciembre 2006, p. 87.

[67] Ortigosa, *op. cit.*, p. 111.

cuentas personales, ayudando al grupo a conseguir más seguidores. O como el grupo CyberCaliphate afiliado a Dáesh, que atacó y tomó el control de las cuentas de Twitter y Youtube del US central Command[68]. Otra de las evidencias ciberyihadistas de Dáesh que existen hoy es la del uso de un código dañino en Siria, con el propósito de obtener datos sobre posiciones de los objetivos locales[69]. Como vemos, estas acciones todavía están lejos de los ciberataques de los que nos venimos ocupando en este trabajo, aquellos que interrumpen o destruyen sistemas informáticos que afectan sectores estratégicos para la población.

5.3. Hacktivismo

El término hacktivismo nació en 1984 debido a un grupo de hackers estadounidense (concretamente en Texas) que adoptaron el nombre de La Secta de la Vaca Muerta (*Cult of the dead cow*), cuyo objetivo era acabar con la censura en internet y ayudar a los internautas que vivían bajo Gobiernos opresivos[70]. El fenómeno engloba la conducta del hacking junto con la del activismo político en internet y refiere la criminalización de la protesta política en internet. Se utiliza el término, sobre todo, para definir a "colectivos antiglobalización y antisistema o que tienen como fin último la desestabilización de un Estado en particular, atacando su estructura social, económica y política, sin olvidar organizaciones clandestinas e incluso acciones encubiertas de las estructuras de inteligencia de algunos Estados"[71]. En definitiva, la cultura hacker, defiende la idea de libertad y neutralidad de internet, donde el grupo más conocido actualmente es el de *Anonymous* o *Wikileaks*[72].

En 2010, Hillary Clinton, proclamó que la *Internet Freedom* sería un eje de su política exterior, cuya finalidad era llevar a la humanidad hacia un proceso irreversible de liberalización política y democratización. Ideales que parecían hacerse realidad en la denominada primavera árabe por la importancia que tuvieron las redes sociales. Destacar también el papel de twitter en 2009 para denunciar el fraude electoral en Irán[73]. Por eso, el "universo del hacktivismo es muy heterogéneo y en él podemos encontrar actores que, a pesar de su praxis delictiva, gozan de una amplia legitimidad por el tipo de objetivos que persiguen"[74]. Hasta aquí todo parecen bondades del ciberactivismo. Sin embargo, en esa diversidad de

---

[68] Villalba Fernández y Corchado Rodríguez, *op. cit.*, p. 114.
[69] *Ibidem* , p. 114.
[70] Torres Soriano, M. R., "El hacktivismo como estrategia de comunicación. De Anonymous al Cibercalifato", en *Cuadernos de Estrategia, núm. 197*, 2018, p. 201.
[71] Ortigosa, *op. cit.*, p. 108.
[72] Miró Llinares, *op. cit*., p. 136.
[73] Torres Soriano, *op. cit.,* p. 199.
[74] *Ibidem* , p. 200.

actores y haciendo uso de la libertad que proporciona internet, también se podrían incluir grupos catalogados como terroristas por Occidente y es aquí cuando comienza la criminalización de la protesta política en internet, sobre todo cuando se trata de la propaganda del cibercalifato, expandiendo así el concepto de ciberterrorismo.

El grupo libertario más conocido en internet hasta ahora es Anonymous. Nació en 2003 creado originariamente como un lugar para el intercambio de archivos de imagen entre los aficionados al anime japonés, pero se consolidó en 2008 al filtrar un video en internet protagonizado por el actor Tom Cruise donde reflexionaba sobre su experiencia como miembro de la cienciología[75]. También ha protagonizado acciones denegación de servicio, por ejemplo, cuando en 2010 el Parlamento australiano proponía una ley para el filtrado de internet, miembros de Anonymous cortaron el acceso a la página del Parlamento[76]. Otras acciones en EEUU, impidieron el acceso a las webs de la Asociación americana de la industria musical y de la Asociación americana cinematográfica, en protesta por los ataques DOS que algunas empresas de contenidos musicales habían llevado a cabo contra webs de intercambio gratuito de archivos[77]. Incluso en España se ha tratado de enjuiciar a la cúpula de Anonymous por tratar de llevar a cabo un ataque informático de Denegación de servicios distribuido (DDos) a la web de la Junta Electoral Central (JEC) y la del Congreso en mayo de 2011 durante la celebración de elecciones autonómicas y locales[78].

Pero quizás, el caso que más le ha dado a conocer sea el del robo de los archivos digitales de la empresa de análisis geopolítico Stratfor. Fue entonces, cuando Anonymous recurrió a los servicios del portal de filtraciones *Wikileaks* liderado por Julian Assange, para poder analizar el contenido de los 2,7 millones de correos electrónicos que habían conseguido extraer de sus servidores, y que ponían en relación intercambios de esta empresa con Gobiernos y empresas de todo el mundo[79]. En definitiva, el principal legado de Anonymous ha sido el haber convertido al hacktivismo en una práctica popular que trasciende el ámbito hacker[80].

Torres Soriano se pregunta sobre la relación entre el hacktivismo y el terrorismo yihadista recordando un vídeo de 2011 elaborado por Al Qaeda titulado: "No confíes en otros, toma la responsabilidad por ti

[75] *Ibidem* , p. 207.
[76] Miró Llinares, *op. cit.*, p. 251.
[77] *Ibidem* , p. 63.
[78] El Juzgado de los penal núm. 3 de Gijón, por sentencia de 6 de Julio de 2016 absolvió a los tres acusados por falta de pruebas. Consultar la sentencia en http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Sala-de-Prensa/Notas-de-prensa/Absueltos-los-tres-acusados-de-ser-la-cupula-de-la-red-Anonymous-en-Gijon (Último acceso: 29 enero de 2021).
[79] Torres Soriano, *op. cit.*, p. 212.
[80] *Ibidem* , p. 213.

mismo", que incitaba a que cualquier musulmán con conocimientos especializados llevase a cabo, "en armonía con el plan general de los muyahidín,… ataques contra los websites y las redes electrónicas de las grandes empresas y las administraciones públicas de los países que atacan a musulmanes"[81]. De alguna manera, la posible existencia de este cibercalifato, está inspirada en la existencia de Anonymous donde "el caso más destacado es el del británico de origen pakistaní Junaid Hussain. Siendo un adolescente creó junto a un amigo un grupo denominado Team Poison con una clara orientación propalestina. A través de su apodo Trick se movería en la órbita de Anonymous con quien compartiría varias ofensivas de hacking, como Operation Free Palestine que apuntó hacia el sistema financiero de Israel en 2011. En 2012, fue condenado a seis meses de prisión por el hackeo de la agenda de contactos del asistente del primer ministro británico Tony Blair así como por realizar más de cien bromas pesadas en la línea de teléfono habilitada por el Gobierno para recibir denuncias contra individuos relacionados con actividades terroristas"[82]. Su estancia en prisión le transformó y en 2014, reaparecería en los territorios dominados por Estado Islámico en Siria, convirtiéndose en el líder del hacktivismo yihadista del Cibercalifato, protagonizando el hackeo del perfil en Twitter del Comando Central del Ejército de los Estados Unidos (CENTCOM) y liderando una nueva denominación del hacktivismo yihadista con el nombre de Islamic State Hacking Division (ISHD)[83].

Actualmente, "el yihadismo continúa siendo uno de los principales motores del hacktivismo. El elemento diferenciador se halla en su vinculación ideológica con los grupos e individuos que emplean la violencia terrorista, lo que otorga un nuevo sentido a muchas de sus actividades"[84]. También existen otros grupos hacktivistas con configuración islamista que sirven de apoyo a Dáesh[85]. Al igual que se ha demostrado que muchos países latinoamericanos han recibido una ofensiva hacktivista constante, como el de Nicolás Maduro en Venezuela[86].

6. Instrumentos internacionales vs código penal: ¿qué se protege?

Hasta ahora se ha tratado de poner de manifiesto una realidad criminal que empieza a desplegarse en el ciberespacio con consecuencias

[81] *Ibidem* , p. 216.
[82] *Ibidem* , p. 218.
[83] *Ibidem* .
[84] *Ibidem* , p. 219.
[85] Villalba Fernández y Corchado Rodríguez, *op. cit.*, p. 117.
[86] *Ibidem* .

que van más allá del daño o la integridad y disponibilidad de datos o sistemas informáticos individuales, llegando a afectar servicios básicos para la ciudadanía. Por tanto, a partir de ahora abordaremos cómo se recoge tal realidad en los instrumentos internacionales existentes y cómo se ha trasladado a nuestro ordenamiento penal. En definitiva, se trata de comprobar si la regulación penal del fenómeno debe quedar circunscrita a daños materiales de carácter individual o si, por el contrario, debe apuntar mejor en la dirección del tipo de ataques como los manifestados hasta ahora en el trabajo.

En primer lugar, el origen de la regulación internacional siempre debemos situarla en el Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Dentro del mismo, el sabotaje se ubica dentro del grupo de delitos contra la integridad y disponibilidad de los datos y sistemas informáticos. Un grupo de delitos que tiene su desarrollo a nivel europeo en la Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005, *relativa a los ataques contra los sistemas de información* y, posteriormente en la *Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo*. Según lo dispuesto en los instrumentos anteriores, el fenómeno que nosotros venimos denominando sabotaje a los datos informáticos adopta la más variada terminología. Así, el Convenio de Budapest recoge en su art. 4 el delito de atentado contra la integridad de los datos, definiéndolo como la "comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos", dejando así al arbitrio de los estados la necesidad o no de que esos actos provoquen daños graves, un aspecto clave en la tipificación de este delito en España. Las mismas conductas que la DM de 2005 denomina intromisión ilegal en los datos (art. 4) y la Directiva de 2013 interferencia ilegal en los datos (art. 5). A diferencia del primero, estos dos últimos instrumentos sí exigen el elemento de la gravedad. En lo que respecta al fenómeno que nosotros hemos denominado sabotaje en el sistema informático, el Convenio de Budapest lo refiere como atentados contra la integridad del sistema (art. 5). Siguiendo el Informe explicativo al Convenio, se trata de aquellas conductas que obstaculizan de manera deliberada el uso legítimo de los sistemas informáticos, incluidos los servicios de telecomunicaciones utilizando o influenciando los datos informáticos donde lo que se protege es el interés de los operadores y los usuarios de los sistemas informáticos o de telecomunicaciones en su funcionamiento correcto[87]. Esta explicación aporta un dato muy importante en el entendimiento de lo que en verdad quiere protegerse con la tipificación de estos delitos desde la esfera internacional, que en ningún caso puede

[87] Informe Explicativo del Consejo de Europa al Convenio sobre Ciberdelincuencia, (STE, núm. 185) 2001, párrafos 65-70.

identificarse con un daño material. Conductas también denominadas como intromisión ilegal en los sistemas de información (art. 3 DM 2005) o interferencia ilegal en los sistemas de información (art. 4 Directiva 2013). Una vez más la gravedad será un aspecto clave a tener en cuenta para separar los casos típicos de los atípicos.

Siguiendo las instrucciones internacionales, nuestro legislador desde 2010 estimó oportuno tipificar y sancionar en artículos separados las conductas ilícitas dirigidas contra datos informáticos, programas informáticos y documentos electrónicos ajenos, de aquellas otras cuyo objeto fuera obstaculizar o interrumpir el normal funcionamiento de los sistemas informáticos. Desde la reforma de 2015, las primeras se recogen en el art. 264 y en el 264 bis los delitos relativos a los daños sobre sistemas informáticos[88]. Hasta aquí todo parece correcto, sin embargo, no se acierta a entender la decisión del legislador de mantenerlas dentro de los delitos contra el patrimonio y el orden socioeconómico. Una decisión que desde el principio no ha estado exenta de dificultades puesto que se trata de un bien jurídico anclado en la propiedad individual ajena, cuando en verdad la tutela de los sistemas de información "no es solo la tutela de un patrimonio individual, por mucho que las conductas que puedan afectar intereses de este carácter se asemejen a las que hacen peligrar infraestructuras críticas que tiene en cuenta la Directiva de 2013"[89]. En verdad, recordemos que estas nuevas conductas según los instrumentos internacionales analizados refieren la integridad de los datos y los sistemas, porque lo que protegen es el interés de los operadores y los usuarios de los sistemas informáticos o de telecomunicaciones en su funcionamiento correcto. Unas dificultades que se hacen más evidentes si partimos de la fenomenología que venimos describiendo sobre sabotaje informático a infraestructuras críticas.

Si tomamos en consideración la decisión de nuestro legislador, debemos interpretar estos delitos en clave patrimonial. Su acercamiento podemos hacerlo desde la tesis económica o desde una tesis funcional. Seguir la tesis jurídico-económico implicaría tomar en consideración únicamente la pérdida del valor del objeto material, lo cual en estos supuestos está claro que carece de sentido. Pareciera más ajustado a los casos que venimos manejando la tesis funcional del daño al captar mejor la realidad que dibujan estos ataques más graves, cuyo objetivo no es solo alcanzar sistemas particulares sino servicios básicos como la energía, el agua, etc., donde lo que está en juego no es el valor de los datos o los sistemas en sí mismos, sino la función que desempeñan para la sociedad. De forma que lo que preocupa no es tanto la pérdida de valor

[88] Circular 3/2017 de la FGE, de 21 de septiembre, *sobre la reforma del Código Penal operada por la LO 1/2015*, de 30 de marzo, cit., p. 20.

[89] De La Mata Barranco, N. J., "La tipificación de los denominados daños informáticos", en *Revista de Derecho penal,* núm. 26, 2018, p. 269.

de los datos o los sistemas sino la integridad y disponibilidad de la información[90]. En esta misma línea, Mazuelos aboga por una concepción del objeto jurídico alejada de la idea naturalística de los daños identificada con lesión corporal de un bien decantándose por una noción normativa que pivote sobre la funcionalidad del bien[91]. En verdad, en los últimos años ni siquiera esta tesis funcional tiene sentido ante la realidad que se impone. Es por eso, que la literatura especializada critica cada vez con más fuerza el mantenimiento de estas novedosas figuras en una rúbrica tradicional del código penal, sin abordar un debate más profundo. Entienden mejor opción llevar estos ciberdelitos a una ubicación sistemática propia que recoja "como bien jurídico lo que ahora supone para el ciudadano no solo la información sino también el uso del ordenador"[92]. Por tanto, ni siquiera hablaríamos de integridad y accesibilidad sino que lo que nos preocupa es el acceso a "un mundo virtual seguro que evite importantes perjuicios para el desarrollo social y personal de una ciudadanía que necesita de él[93]. Es por todo ello que se plantea la necesidad de creación de un bien jurídico nuevo, que no es otro que la seguridad en los sistemas de información[94]. El reto está obviamente en cómo manejar nuevos bienes jurídicos sin renunciar a los principios fundamentales del Derecho penal como el de lesividad o intervención mínima.

En definitiva, la opción que ha tomado el legislador ubicando estas conductas en la rúbrica de los delitos contra el patrimonio y el orden socioeconómico no está exenta de problemas, al no enfocar los casos más graves que son los que parecen referir los instrumentos internacionales, por mucho, como veremos, que el legislador haya introducido el criterio de la gravedad en el tipo penal.

---

[90] De la Mata Barranco y Hernández Díaz, *op. cit.*, pp. 331-333.

[91] Mazuelos Coello, J., "Consideraciones sobre el delito de daños informáticos, en especial sobre la difusión de virus informáticos", en *Derecho penal y Criminología: Ejemplar dedicado a Memorias XXIX Jornadas internacionales de Derecho penal. Informática y Derecho penal. Segunda parte*, Vol. 28, núm. 85, 2007, p. 31.

[92] Adán Del Río, C., "Delitos relativos a los consumidores, delitos informáticos y delitos contra la Hacienda pública", en *Cuadernos penales Jose María Lidón: El anteproyecto de modificación del código penal de 2008. Algunos aspectos,* núm. 6, Universidad de Deusto, 2009, p. 192.

[93] Muy crítico al respecto se muestra en sus reflexiones finales De La Mata Barranco, *op. cit*.

[94] González Hurtado, J. A., "Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: la seguridad en los sistemas de información", en *Revista de Derecho penal, procesal y penitenciario*, núm. 107, 2014, p. 8.

7. Regulación nacional

7.1. La reforma penal de 2010: penalización del sabotaje como delito autónomo

Como ya se ha adelantado, los delitos de sabotaje de datos informáticos y de sistemas informáticos propiamente se introdujeron por primera vez en el código penal español en 2010. Con anterioridad a la reforma, el entonces denominado delito de daños a los elementos lógicos se encontraba regulado en el art. 264.2 CP y parecía constituirse como una mera agravación del delito de daños[95] atendiendo a la peculiar naturaleza del objeto material, quedando "circunscrito a los daños en los elementos lógicos o inmateriales de un sistema informático (software[96]); en consecuencia, los causados en los elementos materiales o físicos (hardware) constituirían un delito básico de daños previsto en el art. 263 CP"[97].

El legislador, en la Exposición de motivos de la LO 5/2010, de 22 de junio por la que se modifica el código penal, justificaba la reforma del art. 264 CP al verse obligado a cumplir "con lo dispuesto por la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información,… que en lo relativo a los daños, quedarían incluidas tanto las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno". Es decir, aseguraba la transposición de Decisión Marco de 2005 relativa a los ataques contra los sistemas de información sin mencionar el Convenio sobre Cibercriminalidad, pese a que este último fue ratificado por España precisamente en junio de 2010 y la Decisión Marco declara tener como base el Convenio citado. Por ese motivo, no deben existir inconvenientes para vincular el nuevo artículo también con este instrumento a los efectos oportunos[98].

---

[95] Respecto del debate sobre si el art. 264.2 CP antes de la reforma de 2010 se constituía como un tipo agravado o como un delito independiente del de daños, consultar De La Mata Barranco y Hernández Díaz, *op. cit.*, p. 324-325. También Morón Lerma, *op. cit*., pp. 117-118.

[96] Andrés Domínguez, A. C., "Comentario previo a los artículos 264, 264 bis, 264 ter y 264 quater", en Gómez Tomillo, M. (dir.), *Comentarios prácticos al Código penal, Tomo III, Delitos contra el Patrimonio y socioeconómicos,* Aranzadi, Pamplona, 2015, p. 347.

[97] Andrés Domínguez, A. C., "Los daños informáticos en el Derecho penal europeo", en Álvarez García, F. J., *La adecuación del Derecho penal español al ordenamiento de la Unión Europea. La Política criminal europea,* Tirant Lo Blanch, Valencia, 2009, pp. 415-416.

[98] En este sentido se expresa la doctrina respecto de la inclusión de otros ciberdelitos en el código penal en 2010, ver Anarte Borrallo, E. y Doval Pais, A., "Límites de la ley penal a propósito del nuevo delito de intrusión informática", en *Revista General de Derecho penal,* núm. 18, 2012, p. 10.

En definitiva, desde la reforma de 2010, dando cumplimiento al mandato internacional, se tipifica como novedad el sabotaje de datos informáticos en el art. 264 CP en su ap. 1 y, en su ap. 2 el sabotaje informático propiamente. De esta forma se constituyen como delitos independientes pero relacionados[99]. Concretamente, el delito de daños de datos informáticos quedaba redactado de la siguiente manera en el art. 264.1 CP: "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". Mientras que el delito de daños a sistemas del art. 264. 2 CP lo hacía así: "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".

Lo cierto es que la aplicación de estos delitos bajo esta regulación no tuvo demasiado recorrido jurisprudencial. Destacan dos casos de distribución de virus *ransomware* durante 2011 y juzgados en la AN en 2016. Se trata del caso conocido como "virus de la policía" por la dinámica que siguieron los ciberdelincuentes. En los sistemas atacados aparecía el siguiente mensaje: "La POLICIA ESPAÑOLA. Atención!!! Ha sido detectada actividad ilegal!! Su sistema operativo ha sido bloqueado debido a una infracción de la legislación española! Han sido detectadas las siguientes infracciones: Su dirección IP ha sido registrada en las webs ilegales con contenido pornográfico orientadas a la difusión de la pornografía infantil, zoofilia e imágenes de violencia contra menores! En su ordenador han sido detectados los archivos de video de contenido pornográfico con elementos de violencia y pornografía infantil! Además, desde su ordenador se realiza un envío ilegal (SPAM) de orientación pro terrorista. El presente bloqueo ha sido realizado para prevenir la posibilidad de difusión de dichos materiales desde su ordenador en Internet. Para desbloquear su ordenador, usted debe pagar una multa de 100 euros! La multa tiene que ser pagada antes de 24 horas desde el momento del bloqueo de su ordenador! En el caso de impago, todos los datos de su ordenador serán eliminados!"[100]. A continuación se les ofrecía la información de cómo

[99] Salvadori, A., "Los nuevos delitos informáticos introducidos en el código penal español con la Ley Orgánica 5/2010", en Pérez Álvarez, F., *Delito, pena, política criminal y tecnologías de la información y la comunicación en las modernas Ciencias penales*, Ediciones Universidad de Salamanca, 2012, pp. 39-42.

[100] Sentencia de la AN (Sala de lo penal, secc. 4º) núm. 14/2016 de 3 de marzo y sentencia de la AN (Sala de lo penal, secc. 4ª) núm. 28/2016 de 4 de julio, que complementa el caso anterior con un acusado al que se le extraditó desde Georgia porque participó en la misma dinámica comisiva con los otros acusados.

abonar esa multa de 100 euros. En este caso se juzgó a varios ciudadanos rusos, quienes desde 2011 y utilizando la dinámica descrita habrían atacado a usuarios de varios países habiendo más de 300 afectados en España. Lo que se pide, entre otros delitos, es la aplicación del entonces art. 264. 2 CP entendiendo que el virus lo que hacía era obstaculizar o interrumpir el funcionamiento del sistema atacado[101].

El segundo lugar, se puede destacar el ya mencionado caso del enjuiciamiento en España a la cúpula de Anonymous. Varias personas fueron acusadas de llevar a cabo un ataque informático de Denegación de servicios distribuido (DDos) a la web de la Junta Electoral Central (JEC) y la del Congreso en mayo de 2011, que hubiera afectado de forma importante al normal funcionamiento del correo electrónico, obstaculizando los trámites previos al proceso electoral y ocasionado el bloqueo de la página web de la Junta electoral central. Así como de perpetrar otro ataque de Denegación de Servicio Distribuido (DDoS) con la llamada operación "V de Votaciones" contra las páginas web del PP, del PSOE y de CIU[102]. El MF acusó por el delito del art. 264.2 CP, aunque finalmente los acusados quedaron absueltos por la falta de pruebas.

7.2. La reforma de 2015

7.2.1 Sabotaje de datos informáticos: tipo básico del art. 264 CP

Como vimos, en Europa, la Decisión Marco 2005/222/JAI del Consejo fue sustituida por la Directiva 2013/40/UE del Parlamento europeo y del Consejo, que se transpuso a nuestro ordenamiento mediante la LO 1/2015 de 30 de marzo y, por la que se modificó el código penal. Después de 2015, el delito de daños de datos informáticos o de interferencia ilegal en los datos queda recogido en el art. 264 CP manteniendo el mismo contenido que en 2010.

El objeto material lo constituyen los datos, ficheros, documentos o programas de software, todos ellos elementos lógicos de un sistema informático. Se trata de un objeto de naturaleza inmaterial que puede definirse como un flujo electromagnético[103]. Recordemos que parte de la doctrina entiende que en el sabotaje a los datos se estaría valorando

[101] Para más información Maeztu, D., "Tipificación penal del ransomware", en Del Derecho y las normas, 2017. Puede consultarse en https://www.derechoynormas.com/2017/05/tipificacion-penal-del-ramsomware.html (último acceso: 30 de enero 2021).

[102] El Juzgado de los penal núm. 3 de Gijón, por sentencia de 6 de Julio de 2016 absolvió a los tres acusados por falta de pruebas. Consultar la sentencia en http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Sala-de-Prensa/Notas-de-prensa/Absueltos-los-tres-acusados-de-ser-la-cupula-de-la-red-Anonymous-en-Gijon (Último acceso: 29 de enero de 2021).

[103] Andrés Domínguez, *op. cit.*, p. 350.

no tanto el daño al dato sino su valor contextual, funcional, dentro del sistema o para la información que representa[104].

Las conductas típicas son las que recogen tanto la DM 2005 como la Directiva de 2013. Se castiga a quien, por cualquier medio, sin autorización y de manera grave, borre, dañe, deteriore, altere, suprima o haga inaccesibles datos o programas informáticos o documentos electrónicos. Con todos estos verbos, el legislador abarca tanto las conductas que impliquen la destrucción, bien total o parcial del objeto material, como aquellas que solo supongan una alteración de los elementos informáticos, ya sea por eliminación, supresión o borrado parcial del elemento afectado o por la incorporación de nuevos datos que varíen el alcance o contenido inicial de esos elementos[105]. Por tanto, se trata de un delito de medios que van desde el borrado manual a la utilización de virus actuando siempre sin autorización[106]. Pueden incluirse aquí los *crash programs* (programas de destrucción progresiva) que pueden borrar gran número de datos en un corto periodo de tiempo o los *time bombs* (bombas lógicas de acción retardada), que causan la destrucción de los ficheros, también el *superzapping, cancer rutine* o los *virus programs*, etc.[107]. Lo relevante es la ajenidad del ataque, lo cual implica que si es el propio propietario del software quien ha programado la destrucción de ficheros la conducta no sería típica[108]. Ante la casuística a la que da lugar emplear tantas acciones típicas, un sector doctrinal propone redactar el tipo penal de modo que indique sencillamente dañar de cualquier modo y de esta forma, dejar a la jurisprudencia la concreción en cada caso concreto[109]. Quizás junto con el replanteamiento del bien jurídico, también habría que replantearse las conductas para cerrar más estos tipos penales, desplazando la importancia hacia los resultados causados y no tanto a las conductas realizadas.

Del análisis de las conductas típicas resulta fácil deducir que exceden de la perspectiva tradicional del concepto de daño[110]. Una problemática que ya se puso de manifiesto en otra parte del trabajo. En relación con lo anterior, se exige que el resultado sea grave, pero también se insiste en que la conducta lo sea, resultando redundante esa doble alusión a la gravedad[111]. Por ello nos hacemos eco de la opinión de la doctrina especializada

---

[104] Morales Gacía, O., "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas" en Quintero Olivares, G. (dir.), *La Reforma penal de 2010: Análisis y comentarios,* Aranzadi-Thomson, Madrid, 2011, p. 189.

[105] Circular de la FGE 3/2017 de 21 de septiembre, *sobre la reforma del Código penal operada por LO 1/2015, de 30 de marzo*, cit., p. 21.

[106] Gómez Rivero, M. C. (dir.), *Nociones fundamentales de Derecho penal (Vol. II) Parte Especial*, Tecnos, Madrid, 2015, p. 196.

[107] Andrés Domínguez, *op. cit.*, p. 353.

[108] *Ibidem* , pp. 351 y 353.

[109] Adán Del Río, *op. cit.*, p. 196.

[110] De La Mata Barranco, *op. cit.*, p. 260.

[111] Castro Corredoira, M. y Vázquez-Portomeme Seijas, F., "La reforma de los delitos de daños: arts. 263, 264, 264 BIS, 264 TER, 264 QUÁTER, 265, 266.1, 266.2 CP", en Cussac,

cuando afirma que lo importante no es el tipo de conducta que se lleve a cabo sino sobre todo cuál sea su consecuencia[112]. Por tanto, no se sancionan las órdenes de ejecución de borrado con independencia del resultado, lo que lleva a plantearnos si lo anterior implica la destrucción de la esencia de la cosa, bien del dato, programa o sistema informático[113]. En los primeros años sí se planteaba la necesidad de que esa alteración, destrucción, inutilización, daño, etc., comportaran una alteración definitiva de la integridad de los datos, programas informáticos o documentos electrónicos, haciendo imposible la utilización o restauración tal y como estaban antes de la realización de la conducta[114]. En los últimos años se ha producido una evolución en el criterio de la gravedad. En verdad, exigir que el resultado sea grave no implica que el objeto no pueda volver a utilizarse de modo absolutamente similar a como se usaba antes del ataque producido, sin pérdida de sustancia ni funcionalidad o, al menos así parece desprenderse de los instrumentos internacionales analizados[115]. Aun así, creemos que resulta criticable la utilización de un parámetro tan abierto, que deje su concreción en manos de criterios jurisprudenciales.

Una última cuestión a abordar sería la existencia de copias de seguridad. Cuando el ataque daña, incluso inutiliza algún dato o programa contenido en un sistema informático particular, como una fotografía o una tesis doctoral, por ejemplo, o cualquier otro documento electrónico del que existe copia de seguridad. Aun cuando el tipo exige gravedad en la conducta y en el resultado, al no estar definido cómo medirla, esta persona podría estar cometiendo el tipo básico, pudiendo ser castigado como autor del delio de sabotaje de datos informáticos. De esta opinión es Aboso, para quien la posibilidad de recuperación de datos o documentos en nada modifica la responsabilidad penal[116]. Sin embargo, la mayoría de la doctrina entiende que cuando existen copias de seguridad nos encontraríamos en la realización del delito en grado de tentativa[117]. Concretamente en una tentativa relativamente inidónea al no haber permanencia del daño inicial producido[118].

El delito tampoco ha tenido mucho recorrido jurisprudencial en estos años. Aunque sí cabe resaltar el caso de quien fue contratado para

---

J. L. (dir.); *Comentarios a la reforma del código penal de 2015, 2ª edición, Actualizada con la corrección de errores (BOE 11 de Junio de 2015)*, Tirant Lo Blanch, Valencia, 2015, p. 831.

[112] De La Mata Barranco, *op. cit.*, p. 262.

[113] Morales García, *op. cit.*, p. 190.

[114] González Rus, J. J., "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", en *Revista electrónica de Ciencia penal y Criminología*, núm. 1, 1999.

[115] De La Mata Barranco, *op. cit.*, p. 263.

[116] Esta es la postura de Aboso, G. E., *La criminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*, BdeF, Buenos Aires, 2017, p. 359.

[117] Partidarios de castigar la existencia de copias de seguridad como delito en grado de tentativa son: González Rus, *op. cit*. También Romeo Casabona, *op. cit.*, p. 110.

[118] De La Mata Barranco, *op. cit.,* p. 269.

la creación de una página web y en esa labor acabó apropiándose de ese dominio de internet. En este caso, lo que se juzga es esa imposibilidad por parte del propietario de poder recuperar la titularidad del dominio de su página web y la imposibilidad de tener conocimiento de las claves de acceso (FJ. 3). De todas las conductas descritas en el tipo penal, la que realiza el acusado es la de hacer inaccesibles datos o programas informáticos, que abarca toda acción que obstaculiza de manera permanente o temporal la disponibilidad y la correcta utilización de los datos informáticos por parte del titular del derecho. En definitiva, la conducta desplegada por el acusado provocó que el legítimo titular del dominio no pudiera tener acceso al mismo siendo castigado por el delito del art. 264 CP[119].

7.2.2. El delito de sabotaje a sistemas informáticos: Tipo básico del art. 264 bis CP

Tras la reforma de 2015 el delito se tipifica en el art. 264 bis castigando los ataques a sistemas informáticos[120]. Este delito sí incorpora algunos cambios respecto de la legislación de 2010. El elemento esencial sigue siendo que se produzca la efectiva y grave obstaculización o interrupción de un sistema informático concreto[121]. El nuevo precepto dispone que; "1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo anterior; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado".

Como sabemos, una de las diferencias fundamentales respecto del delito del art. 264 CP radica en el objeto sobre el que recae la acción típica, que en este caso son los sistemas de redes o *hardware* del ordenador/tablet/smartphone, las redes de intranet o las webs de las empresas, las redes informáticas de organismos públicos o privados[122]. En definitiva, los sistemas informáticos, el *hardware*, debiendo quedar fuera las acciones dirigidas contra datos, programas informáticos y documentos

[119] SAP Guipúzcoa (secc.1ª) 120/2019 de 13 de junio.

[120] Gómez Rivero, M. C. (dir.), *Nociones fundamentales de Derecho penal (Vol. II) Parte Especial*, Tecnos, Madrid, 2015, pp. 198-199.

[121] Circular de la FGE 3/2017 de 21 de septiembre, *sobre la reforma del Código penal operada por LO 1/2015, de 30 de marzo*, cit., p. 29.

[122] Gómez Rivero, *op. cit.*, p. 198.

electrónicos, salvo que la interferencia ilegal en ellos fuera el medio para afectar el sistema[123].

Para realizar la conducta típica caben las acciones descritas en el delito anterior (art. 264 CP), siempre que el objeto de la acción no sean datos, programas o documentos, sino los propios sistemas. La conducta debe llevarse a cabo sin autorización y generar resultados graves, que al igual que en el precepto anterior, tampoco se concreta qué debe entenderse por grave, lo cual generará problemas para saber qué conductas serán relevantes para el Derecho penal y cuáles no. En verdad, las dudas sobre alterar, hacer inaccesibles, y el resto de conductas del precepto anterior a las que se refiere el apartado a) aquí no deberían plantearse porque se penaliza la mera obstaculización o la interrupción y no solo el daño definitivo[124]. Por el contrario, reconoce la Fiscalía General del Estado en su Circular 3/2017 que muchos de estos comportamientos podrían reconducirse a las acciones típicas del art. 264.1º CP, por lo que en una pluralidad de ocasiones la aplicación de uno u otro tipo penal vendrá determinada por la capacidad de la acción para afectar a la operatividad o al funcionamiento del sistema informático en su conjunto[125]. En cuanto a las conductas recogidas en el apartado b) referidas a la introducción o transmisión de datos, pudiera resultar complicado diferenciarlas de las comprendidas en el apartado a) en determinados supuestos[126]. Quizás el ejemplo más claro de estas conductas de introducción o transmisión de datos lo constituya el ataque de denegación de servicios, porque produce la interrupción del funcionamiento de un sistema mediante órdenes comunes a una máquina, ejecutadas simultáneamente y de modo masivo[127]. Finalmente, en lo que a conductas se refiere, la novedad principal con respecto a la redacción de 2010, es la introducción de un nuevo modo de interrumpir u obstaculizar el funcionamiento de un sistema informático. Se trata del apartado c) que llega a ese resultado bien destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica que, además, no está previsto en el art. 4 de la Directiva[128].

Existen varias modalidades de ejecución de la conducta, como el mail bomber que bloquea la dirección de correo electrónico del usuario; las bombas ansi, que manipulan el teclado asignado a las teclas funciones diferentes a las habituales; los ataques de denegación de servicios

---

[123] Castro Corredoira y Vázquez-Portomeme Seijas, *op. cit.*, p. 832.

[124] De La Mata Barranco, *op. cit.*

[125] Circular de la FGE 3/2017 de 21 de septiembre, *sobre la reforma del Código penal operada por LO 1/2015, de 30 de marzo*, cit., p. 37.

[126] *Ibidem* , p. 30.

[127] Morales Gacía, *op. cit.,* p. 189.

[128] Andrés Domínguez, A. C., "Artículo 264 bis", en Gómez Tomillo, M.; *Comentarios prácticos al Código penal, Tomo III, Delitos contra el Patrimonio y socioeconómico*s, Aranzadi, Pamplona, 2015, p. 358.

a servidores para que dejen de cumplir su función y obedezcan las órdenes del ciberdelincuente[129]. También, pueden cometerse a través de un adware que impide navegar por el bombardeo de anuncios, o por la introducción de gusanos que provocan que el ordenador vaya más lento. En cambio, los troyanos lo que hacen es proporcionar un acceso no consentido, por lo que no afectan ni al funcionamiento del ordenador ni destruye ficheros y, por ello, su castigo tendría mejor cabida en los delitos contra la intimidad[130].

De un análisis comparado de los tipos penales del 264 y 264 bis se comprueba una mayor gravedad en la obstrucción del sistema que en el ataque a los datos en él contenidos. Así consta en la Circular de la FGE de 2017 cuando afirma que "el legislador ha considerado notablemente más graves y peligrosas, porque así lo son efectivamente, las acciones dirigidas contra el sistema informático en su conjunto que provocan su interrupción u obstaculizan de forma grave su normal funcionamiento, respecto de aquellas otras que afectan exclusivamente a los datos, programas o documentos electrónicos aun cuando tengan incidencia, al menos indirecta, en el sistema en el que se integran, siempre que no impliquen una pérdida significativa en la funcionalidad del mismo"[131].

Consecuencia inmediata de la mayor gravedad del sabotaje al sistema, se plantea la duda de cómo castigar estas conductas si existen copias de seguridad de los datos, programas o documentos electrónicos afectados que obstruyen a su vez el funcionamiento del sistema. En este caso, la doctrina no ve claro su punición en grado de tentativa. Resulta que, quienes apostaban por entender la concurrencia de la tentativa del delito de sabotaje a datos cuando existieran copias de seguridad no ven tan clara la respuesta cuando se eliminan o borran datos de un fichero informático de especial trascendencia para el funcionamiento de una empresa, una Administración pública o una infraestructura crítica. De esta forma, se entiende en estos casos que, cuando se obstruye el funcionamiento de estos sistemas, aunque exista una copia de seguridad, si las copias no se encuentran en la sede física donde se ubica el sistema, o bien su reincorporación al sistema lleva días y, por tanto se paraliza la actividad de esa empresa, la Administración o la infraestructura crítica durante ese espacio de tiempo, debería aplicarse el delito consumado, quedando la tentativa para los casos en los que la instalación de las copias sea posible en poco tiempo[132].

Si efectivamente, como hemos comprobado, las conductas del tipo básico contenidas en el art. 264 bis CP son más graves que las contenidas

[129] *Ibidem* , p. 359.
[130] Gómez Rivero, *op. cit.*, p. 199.
[131] Circular de la FGE 3/2017 de 21 de septiembre, *sobre la reforma del Código penal operada por LO 1/2015, de 30 de marzo*, cit., p. 30.
[132] De La Mata Barranco y Hernández Díaz, *op. cit.,* pp. 353-354.

en el tipo básico del art. 264 CP, nos resulta criticable que las penas destinadas a uno y otro delito sean iguales, castigándose con la misma pena de prisión que va desde los seis meses de prisión a los tres años.

Una vez más, la mayoría de los casos que nos ofrece la jurisprudencia hasta el momento no resultan demasiado ilustrativos, al no quedar suficientemente probados por la dificultad que entraña la investigación de estos delitos. Es el caso de los dos ataques informáticos que una empresa sufrió en febrero de 2018 mediante un virus ransomware, que dejó encriptada su información haciendo imposible la recuperación de los datos[133]. El caso se sobreseyó dada la imposibilidad de averiguar la IP desde la que se produjeron los ataques informáticos, ya que dicha empresa procedió a dar de baja el servidor virtual objeto del ataque, motivo que no permitió continuar con la investigación dirigida a identificar a los responsables. También es destacable un Auto de la AN, referido a la extradición de un ciudadano ruso a EEUU, por la utilización del *botnet Keihlos* que causó especiales consecuencias en el Distrito de Connecticut. Según los hechos probados, el *botnet Kelihos* estuvo controlado por el acusado y le permitió dar órdenes a cualesquier y a todos los bots en el *botnet Kelihos*. El acusado controló y operó esta botnet para, entre otras cosas: (1) recoger información personal y medios de identificación como direcciones de correo electrónico, nombres de usuarios, nombres de acceso y contraseñas de los ordenadores infectados; (2) difundir correo basura y (3) distribuir software malintencionado, incluyendo troyanos y *ransomware*. Los ordenadores infectados afectaron el comercio y las comunicaciones interestatales en el extranjero[134]. Fue extraditado a EEUU para su enjuiciamiento por el delito de daños informáticos (entre otros). El Auto no facilita más información, por lo que no podemos saber si estos hechos podrían ser subsumibles dentro del sabotaje a los datos informáticos o a los sistemas de información conforme a la legislación española.

Mucho más ilustrativo resulta el caso de un investigador que realizaba su tesis doctoral en uno de los laboratorios del Instituto de Biología y Genética molecular, perteneciente a la Universidad de Valladolid y el CSIC. Este investigador adquirió un dispositivo USB killer con el que atacó varios ordenadores de su laboratorio. La función del dispositivo es probar puertos USB contra ataques de sobre tensión de forma que, cuando se conecta al USB de un ordenador, lo que hace es recolectar la energía de las conexiones de alimentación descargando muchos voltios sobre la placa base del ordenador dejándola dañada[135]. El caso resulta interesante pues se debate si esos ordenadores al formar parte de la Administración pública (Universidad de Valladolid-CSIC) cumplen una función

[133] Auto de la AP Barcelona (Secc. 7ª) núm. 526/2020 de 4 de septiembre.
[134] Auto de la AN (Sala de lo penal, secc. 4º) de 3 de octubre de 2017.
[135] Hechos probados de la SAP Valladolid (Secc. 2º) 82/2020 de 8 de junio.

que va más allá del usuario, lo cual se materializaría en la aplicación de una agravación, aunque finalmente la concurrencia de tal agravante se descarta. Sin duda estamos ante el art. 264 bis CP porque la conducta no solo afecta elementos aislados que integran el sistema sino a la operatividad funcional del propio sistema (FJ. 5). Por tanto, se descarta que el objeto material en este supuesto fueran los datos o programas informáticos, o los documentos electrónicos, entendiendo que el precepto susceptible a aplicar en el caso debía ser el art. 264 bis CP (FJ. 8). El resultado grave consistió en la obstaculización o interrupción del funcionamiento de un objeto material, en este caso además fueron más de veinte sistemas informáticos ajenos los atacados (FJ. 9)[136].

7.2.3. Tipo agravado: afectación de una infraestructura crítica

Como novedad, desde 2015, se añaden a los dos tipos penales analizados con anterioridad una serie de agravantes, recogidas en el apartado 2 de los art. 264 y 264 bis CP cuando el sabotaje "se hubiera cometido en el marco de una organización criminal, o bien haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos, o que hubieran perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad". Pero la que nos interesa resaltar aquí fundamentalmente, es la agravante recogida en el punto 4, al referirse a la afección del "sistema informático de una infraestructura crítica o la creación de una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea". A estos efectos, en el mismo párrafo se define infraestructura crítica como "un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones". Especial mención nos merece, por tanto, este punto 4, al referir el ataque a una infraestructura crítica que conlleve una situación de peligro grave para el bienestar de la población, hechos a los que hemos venido haciendo alusión durante toda la primera parte de este trabajo. El debate sobre la ubicación del delito y el bien jurídico protegido toma más fuerza, si cabe, cuando del análisis de las agravantes se trata. En las agravantes carece de sentido hablar de patrimonio y orden socioeconómico y debe valorarse un nuevo bien jurídico más relacionado con la seguridad de los datos y sistemas informáticos[137].

Sin duda alguna, en estas agravantes se recoge la esencia de lo que venían demandando los instrumentos internacionales, quedando los

[136] SAP Valladolid (Secc. 2º) 82/2020 de 8 de junio.
[137] Gómez Rivero, *op. cit.*, p. 199.

tipos básicos muy alejados de la gravedad de los hechos que se predican cuando se afectan servicios básicos para la ciudadanía como la salud, protegiendo el buen funcionamiento de los sistemas sanitarios en plena pandemia del Coronavirus, el buen funcionamiento de los sistemas de energía en plena ola de frío en España, etc.

A modo de reflexión personal, nos quedan algunas dudas por resolver en cuanto a la penalidad de estas conductas. Respecto de la aplicación del art. 264 CP, en el supuesto de que un particular dañe, incluso inutilice, algún dato o programa contenido en un sistema informático particular (una foto o una tesis doctoral por emplear los mismos ejemplos que se emplearon con anterioridad), contenido en cualquier ordenador o smartphone de un particular y, aun cuando el tipo exige gravedad en la conducta y en el resultado, al no estar definido cómo medirla, esta persona podría estar cometiendo el tipo básico, castigándole como autor del delio de sabotaje de datos informáticos (en tentativa o no como vimos), pudiendo llegar la pena, desde los seis meses de prisión a los tres años. Por el contrario, si esta persona, con su acción, afectase a los datos contenidos en un sistema que soporta una infraestructura del Estado o de la Unión europea, como la salud, el agua, o la energía, etc, la pena a imponer estaría entre los dos y los cinco años de prisión. En verdad, no parecen penas proporcionadas a la gravedad de los hechos, pues ambas horquillas penales comparten el tramo que va desde los dos a los tres años, pudiendo castigar a los autores de acciones y consecuencias tan diferentes para los derechos básicos de la población, con penas muy parecidas, o incluso iguales. En nuestra opinión, no se trata de castigar más duramente la segunda conducta, sino de repensar la necesidad del castigo en la primera. Quizás este tipo de sabotaje, pueda encontrar mejor acogida en otras ramas del ordenamiento jurídico como el Derecho administrativo sancionador o en la responsabilidad civil cuando se produzcan daños que sean reparables sin más.

En lo que respecta al art. 264 bis CP, la pena de prisión para quien realice la conducta definida en el tipo básico podría ir desde los seis meses a los tres años de prisión. Mientras que, si ese ataque se llevara a cabo a una infraestructura crítica la pena para el autor podría llegar desde los tres a los ocho años de prisión. En este caso, el límite máximo del tipo básico, coincide justo con el límite mínimo del supuesto agravado, una diferente respuesta penal, para quien sin duda logra un resultado de gravedad muy diferente. Una vez más y, en defensa de principios penales básicos como el de última ratio, según nuestra opinión merecen castigo penal sólo aquellos ciberataques más graves, los que se castigan en las agravantes.

En definitiva, no deja de resultarnos criticable que los tipos básicos del 264 y 264 bis, aun cuando ha quedado demostrado que responden a conductas de gravedad tan diferente, refieran las mismas penas (seis meses a tres años de prisión en ambos casos) y, sin embargo, los tipos

agravados en tanto los ataques alcancen infraestructuras críticas sí se castiguen de forma muy diferente, siendo en el primer caso dos a cinco años de prisión y en el segundo tres a ocho años de prisión. Las penas en las agravantes sí recogen la mayor gravedad del art. 264 bis CP, que debería reflejarse también en el tipo básico.

8. El delito de sabotaje con finalidad terrorista del art. 573.2 CP

8.1. Delitos graves: introducción del sabotaje informático como delito grave

El art. 3 de la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 *relativa a la lucha contra el terrorismo* insta a los estados a tipificar con arreglo al Derecho nacional "actos que, por su naturaleza o contexto pueden perjudicar gravemente a un país o a una organización internacional", especificando, en su apartado d) las conductas de "destrucciones masivas de instalaciones estatales o públicas, sistemas de transporte, infraestructuras, sistemas informáticos incluidos". También en su apartado i) remite al delito de "interferencia ilegal en los sistemas de información a tenor del artículo 4 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, en los casos en los que sea de aplicación su artículo 9 …, apartado 4, letra c)". Este último apartado (art. 9. 4 c. de la ya mencionada Directiva de 2013) es precisamente el que refiere a que esa interferencia ilegal en los sistemas *se cometa contra el sistema de información de una infraestructura crítica.* Es decir, esta Directiva pone el énfasis precisamente en aquel sabotaje que es capaz de afectar al funcionamiento del sistema informático de una infraestructura crítica, no a cualquiera sistema.

Con carácter general, la técnica de tipificación del terrorismo en los países de nuestro entorno responde a dos modelos básicos; el modelo estrictamente objetivo y el modelo subjetivo-objetivo[138]. Por un lado, ambos modelos comparten la técnica de enumeración de delitos graves, esto es, los delitos contra la vida, la integridad, libertad, daños, estragos, etc. En este sentido, el legislador español de 2015, añade al listado clásico de delitos, los delitos de sabotaje informático de los artículos 264 y 264 BIS CP. Por otro lado, la diferencia fundamental de estos modelos radica en requerir o no, un elemento subjetivo típico que refiera bien a una finalidad próxima, como intimidar o causar terror, o alterar gravemente el

[138] Asúa Batarrita, A., "Concepto jurídico de terrorismo y elementos subjetivos de finalidad. Fines políticos últimos y fines de terror instrumental", en Echano Basaldúa, J. I. *Estudios jurídicos en Memoria de José María Lidón,* Universidad de Deusto, 2002, p. 49.

orden público, o bien haga referencia a finalidades últimas de carácter político[139]. El modelo español, responde al denominado modelo mixto, ya que además de enumerar delitos graves exige la concurrencia del requisito subjetivo de la finalidad política[140].

Efectivamente, de la actual definición de terrorismo en el código penal español, puede desglosarse un elemento material y otro teleológico[141]: El elemento material lo componen los delitos que se referencian en el art. 573.1 CP, de forma que "se considerará delito de terrorismo la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexuales, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, contra la Corona, de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos, previstos en el presente Código, y el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías", a los que en 2015 se añade, en el 573.2 CP que: "se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos … 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior"[142]. Del análisis realizado con anterioridad en este trabajo, queda más o menos acreditada la gravedad de las conductas recogidas en el art. 264 bis CP, máxime cuando alcanzan sistemas referidos a infraestructuras críticas. Pero, nos queda la duda respecto del art. 264 CP. Bajo nuestro punto de vista, quizás sean graves aquellas conductas de sabotaje que alcancen datos contenidos en los sistemas que soportan este tipo de infraestructuras, pero tal gravedad, nunca podría predicarse respecto de las conductas recogidas en el tipo básico. Por eso, el recurso en bloque utilizado por nuestro legislador en el art. 573.2 CP, refiriéndose a los artículos 264 y 264 bis, quizás no sea una técnica legislativa adecuada al carácter de *ultima ratio* del Derecho penal. Entendemos que, hubiera sido preferible, en vez de esta remisión en bloque, haber hecho alusión a los artículos 264. 2 y 264 bis. 2 CP. Hechos que efectivamente, sí revisten una especial gravedad.

En lo relativo al elemento teleológico, la cuestión sobre "la relevancia que debe concederse a la finalidad política en la delimitación de los actos terroristas, ha sido uno de los escollos que durante el siglo pasado frustraron los intentos de una definición internacional de terrorismo"[143].

---

[139] *Ibidem*. Así mismo, Berdugo Gómez De La Torre, I., "El terrorismo en el s. XXI: del Terrorismo nacional al terrorismo global", en *Revista penal, núm. 42,* 2018, p. 21: La falta de una definición internacional se debe al distinto posicionamiento de los Estados respecto de la valoración del componente político del terrorismo.

[140] Asúa Batarrita, *op. cit.,* p. 51.

[141] Cano Paños, M. A., "La reforma penal de los delitos de terrorismo en el año 2015. Cinco cuestiones fundamentales", en *Revista General de Derecho penal,* núm. 23, 2015, p. 6.

[142] *Ibidem*.

[143] Asúa Batarrita, *op. cit.*, p. 52.

Sin embargo, desde los años 90 del pasado siglo, se atisban cambios para poder diferenciar al fin "el derecho a la resistencia y los actos de terrorismo, la delincuencia política contra el Estado, y la violencia política que se cierne de forma indiscriminada sobre sectores de la población"[144]. Logros que vuelven a estar en revisión, porque en los últimos tiempos y, debido sobre todo a las acciones libradas en internet, parece que vuelven a confundirse fenómenos de mera protesta, con acciones terroristas.

8.2. Elemento teleológico del terrorismo

Negar al terrorismo su condición de delito político no implica negar la intencionalidad política de su motivación[145]. Recordemos que los delitos de terrorismo ya están tipificados como delitos comunes en el código penal, pero adquieren la dimensión de terrorista por la finalidad perseguida[146]. El elemento teleológico viene configurado por esa finalidad[147]. Si bien es cierto que, más allá de la finalidad no se puede obviar que una de las características del terrorismo es la gravedad de sus resultados[148], por eso, la mayoría de la doctrina coincide en que son los medios violentos del terrorismo los delictivos y no tanto sus fines[149]. Aunque en verdad nunca se sabrá por qué un terrorista (el motivo) decide cometer un atentado, sí se puede presuponer su intención política en sentido amplio si con ese acto se coacciona al Estado y se proclama esa intención política que hacen que, aunque el motivo esté blindado, la cadena de elementos subjetivos del tipo sea transparente[150]. Por eso el terrorismo muestra cierta contradicción en cuanto a su significado político, porque por un lado en su comunicación pública se reafirma en su carácter delictivo y, por tanto, en la ausencia de elementos políticos, pero por otro lado son delitos diferentes a la delincuencia común porque sus razones son políticas[151]. Atender a esta finalidad política hará posible su diferenciación de los actos propios de la criminalidad organizada, de tal forma que no

---

[144] *Ibidem*.

[145] *Ibidem*, p. 53.

[146] Llobet Anglí, M., "Tema 18. Delitos contra el Orden público", en VV.AA. *Lecciones de Derecho penal. Parte Especial. Cuarta edición adaptada a la LO 1/2015 de reforma del CP*, Atelier, Barcelona, 2015, p. 433.

[147] Cano Paños, *op. cit.*, p. 6.

[148] Fernández Hernández, A., "La reforma penal de 2015 en materia de terrorismo: el ocaso de los principios limitadores del Ius Puniendi", en Cuerda Arnau, M. L. y García Amado, J.A (dirs.), *Protección Jurídica del Orden Público, la paz pública y la seguridad ciudadana*, Tirant Lo Blanch, Colección delitos, 119, Valencia, 2016, p. 119.

[149] Cancio Meliá, M., *Los delitos de terrorismo: estructura típica e injusto*, Ed, Reus, Madrid, 2010, p. 183.

[150] Pérez Caballero, J., "Defensa de los elementos contextual y político de los crímenes de lesa humanidad contra la expansión del tipo al terrorismo internacional", en *Revista electrónica de Ciencia penal y Criminología,* núm. 15, 2013, p. 12.

[151] Cancio Meliá, *op. cit.*, pp. 134-135.

todo recaiga bajo la legislación de excepción terrorista. Para entender estas finalidades atenderemos a lo dispuesto en las Decisiones marco y Directivas europeas existentes hasta el momento.

La primera, la Decisión marco del Consejo de 13 de junio de 2002 sobre la lucha contra el terrorismo (2002/475/JAI) del Consejo De La Unión Europea, establece en su art. 1 que: "Todos los Estados miembros adoptarán las medidas necesarias para que se consideren delitos de terrorismo los actos intencionados a que se refieren las letras a) a i) tipificados como delitos según los respectivos Derechos nacionales que, por su naturaleza o su contexto, puedan lesionar gravemente a un país o a una organización internacional cuando su autor los cometa con el fin de:

— intimidar gravemente a una población,

— obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo,

— o desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales de un país o de una organización internacional".

Los instrumentos posteriores no modifican estas finalidades. No lo hace ni la Decisión Marco 2008/919/JAI del Consejo de 28 de noviembre de 2008 *por la que se modifica la anterior Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo*, ni tampoco, ni tampoco la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 *relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo*[152].

Atendiendo a lo anterior, cabe preguntarse si el código penal español se ajusta a estas finalidades. Pues bien, si hasta el año 2015 se especificaban dos finalidades en el entonces art. 571 CP: "la de subvertir el orden constitucional, y alterar gravemente la paz pública mediante la perpetración de cualquiera de los delitos graves previstos en la sección siguiente" (sección 2ª: De los delitos de terrorismo), a partir de 2015 se amplían. Además, queda remarcado el carácter de excepcionalidad del terrorismo porque si toda la reforma del código penal se llevó a cabo mediante LO 1/2015, la legislación antiterrorista lo hizo por una ley diferente, la LO 2/ 2015 traducida en una suerte de legislación especial

[152] Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo en su art. 3, en su apartado 2 que: "los fines a que se refiere el apartado 1 son los siguientes: a) intimidar gravemente a una población; b) obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo; c) desestabilizar gravemente o destruir las estructuras políticas, constitucionales, económicas o sociales fundamentales de un país o de una organización internacional".

tramitada al margen del resto de la reforma[153] que además, refiere cuatro las finalidades, añadiendo así dos más a las anteriores que son; la desestabilización grave de una organización internacional y la provocación de un estado de terror en la población. Por tanto, el actual art. 573.1 CP establece cuatro finalidades:

> "1.ª Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.
> 2.ª Alterar gravemente la paz pública.
> 3.ª Desestabilizar gravemente el funcionamiento de una organización internacional.
> 4.ª Provocar un estado de terror en la población o en una parte de ella".

Como ya se ha puesto de manifiesto, partimos de que el actual concepto jurídico penal de terrorismo queda vinculado al elemento político, siendo precisamente ese elemento el que convierte algunas organizaciones criminales y delincuentes en específicamente terroristas[154]. El problema viene dado en la excesiva amplitud de estas finalidades en España que no atienen a un criterio de gravedad propio de los delitos de terrorismo como pasamos a comprobar, lo que deja abierta la posibilidad de una interpretación extensiva.

Respecto de la primera de las finalidades, la de "subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo", es fácil deducir cómo los términos empleados son jurídicamente indeterminados; "suprimir, desestabilizar gravemente el funcionamiento de las instituciones políticas, o estructuras económicas o sociales del Estado". Lo anterior atenta contra el mandato de taxatividad derivado del principio de legalidad, delegando la tarea de concreción a la Audiencia Nacional y al Tribunal Supremo que tendrán que ir llenando de contenido tales expresiones[155]. En verdad, esta finalidad no solo puede predicarse de los terrorismos nacionales sino también del terrorismo internacional. Por ejemplo, subvertir el orden constitucional se constituye como un fin político que puede trascender nuestras fronteras si pensamos en la finalidad del terrorismo islámico, que pude englobar cualquier otra finalidad política que persiga un ente asociativo con sus acciones violentas[156]. De esta forma,

---

[153] Navarro Cardoso, F., "El delito de financiación del terrorismo en el código penal español (art. 576 CP", en Ferré Olivé J. C. Y Pérez Cepeda, A. I. (dirs.); *Financiación del Terrorismo,* Tirant Lo Blanch, Valencia, 2018, p. 81.

[154] Cancio Meliá, *op. cit.,* pp. 135-136.

[155] Fernández Hernández, *op. cit.*, p. 138.

[156] Capita Remezal, M., *Análisis de la legislación penal antiterrorista,* Colex, Madrid, 2008, p. 51.

si el terrorismo entraña el propósito específico de atentar contra el sistema democrático también puede hacerlo contra todo el sistema occidental, esto es, contra los cimientos políticos, culturales o religiosos como es el caso del terrorismo islámico[157]. Así, el Grupo de Estudios de Política Criminal acepta que el fin último del terrorismo integrista islámico también es político, aunque sus acciones "se presenten en ocasiones como actos concretos de represalia o de propaganda[158]". Por ello, coincidimos con el criterio del mencionado Grupo cuando propone sustituir la tradicional finalidad relativa a la de "subvertir el orden constitucional", por la referencia a "fines políticos contrarios al sistema democrático[159]". En este sentido también parecía pronunciarse la sentencia de la Audiencia Nacional 65/2007 de 31 de octubre, por los atentados ocurridos en Madrid el 11 de marzo de 2004 al entender que los miembros de estas células o grupos terroristas de tipo yihadista, pretendieron "mediante el uso de la violencia en todas sus manifestaciones, derrocar los regímenes democráticos y eliminar la cultura de tradición cristiano-occidental sustituyéndolos por un Estado islámico bajo el imperio de la Sharia o Ley islámica en su interpretación más radical, extrema y minoritaria"[160].

En lo que respecta a la segunda finalidad, la de *alterar gravemente la paz pública*, puede decirse que dicha alteración, no es en realidad una finalidad sino un resultado mismo de la acción terrorista[161]. Además, no está recogida en los instrumentos internacionales[162]. En realidad, alterar gravemente la paz pública equivale a la creación de una alarma en la colectividad, que no es más que un resultado inmediato de la actividad terrorista[163]. Volviendo a los atentados del 11 M de 2004 en Madrid, determinados autores que, incluso antes de que se pronunciase la AN en los términos ya referidos, entendían que aquellos tentados del 11 M estuvieron encaminados a la modificación de la política exterior española[164]. Por su parte Lamarca, afirma que la alarma debe entenderse como un fin inmediato de la actuación terrorista porque, si no se requiere esa finalidad política, entonces será muy difícil distinguir el terrorismo de otros tipos delictivos como los desórdenes públicos[165]. Por todo lo anterior, debido a

---

[157] *Ibidem*, p. 54.

[158] Grupo De Estudios De Política Criminal, "Una alternativa a la actual Política Criminal sobre terrorismo", *Documentos 9*, 2008, p. 25.

[159] *Ibidem*, p. 25.

[160] SAN 65/2007 de 31 de octubre.

[161] Capita Remezal, *op. cit*., p. 51.

[162] Críticamente con su referencia en el ámbito nacional, García Rivas, N., "Delitos de atentado, resistencia y desobediencia", en Quintero Olivares, G. (dir.); *Comentarios a la Reforma penal de 2015*, Aranzadi, Pamplona, 2015, p. 776.

[163] Capita Remezal, *op. cit*., p. 53.

[164] Jordán, J., "El terrorismo islamista en España", en Blanco Abarca, A., Del Aguila Tejerina, R. y Sabucedo Cameselle, J. M. (coords.), *11-M: un análisis del mal y sus consecuencias* Ed. Trotta, Madrid, 2005, pp. 79-112. Citado por Cancio Meliá, *op. cit.*, p. 187.

[165] Lamarca Pérez, C., "Análisis de las reformas penales: el caso español", en Serrano-Piedecasas, J. R.; Demetrio Crespo, E. (dirs), *Terrorismo y Estado de Derecho,* Iustel, Ma-

las dificultades derivadas de esta finalidad, el Grupo de Estudios de Política Criminal apuesta por la supresión de la misma por atentar contra el principio de legalidad y porque el mantenimiento de dicha cláusula niega el carácter político del terrorismo y lo hace difícil de diferenciar respecto del delito de desórdenes[166]. Lo complicado es limitar el concepto "paz pública" y, de no hacerlo, pueden entrar dentro colectivos que no necesariamente revisten un carácter ilícito[167] como en el caso del ciberespacio pueden ser *Anonymous* o *Wikileaks*.

Pues bien, lejos de hacer caso a estas recomendaciones del Grupo de Estudios de política criminal, nuestro legislador en 2015, no solo no derogó esta cláusula sino que decidió añadir otras dos, que son la *desestabilizar gravemente el funcionamiento de una organización internacional*, y la de *provocar terror en la población,* finalidades también profundamente amplias. Entendemos que, un concepto estricto de terrorismo no puede permitirse las finalidades más allá de lo estrictamente político. Por eso, coincidimos con Pérez Cepeda cuando afirma que, *stricto sensu*, finalidades políticas son la primera y la tercera de las recogidas en el art. 573.1 CP[168] y, aun así, suprimiría la tercera, relativa a la desestabilización grave de una organización internacional por dos motivos principalmente; en primer lugar porque no distingue entre organización internacional pública u organización intergubernamental (OIG) y organización internacional privada u organización no gubernamental (ONG) y, aun así, aunque se limitara a las primeras, todas ellas adolecen de un déficit democrático y no ejercen un modelo de gobierno internacional a través de asambleas o parlamentos. En segundo lugar, por lo indeterminado que resulta la utilización de "desestabilizar gravemente", puesto que nunca será un objetivo terrorista pretender hacer cambiar algunas de sus políticas, que además por el ámbito territorial se hace imposible[169].

La última de las finalidades referida a la provocación de terror, no es más que un efecto concomitante al empleo de violencia grave, en el marco de una estrategia política llevada a cabo por parte de una organización[170], por lo que, se propone la supresión de esta finalidad[171], como ya se propuso la supresión de la alteración de la paz pública por el mismo motivo.

---

drid, 2010, p. 439.

[166] Grupo De Estudios De Política Criminal, "Una alternativa a la actual Política Criminal sobre terrorismo", *Documentos 9*, 2008, p. 26.

[167] Fernández Hernández, *op. cit.*, p. 137.

[168] Pérez Cepeda, A. I., *El Pacto antiyihadista: criminalización de la radicalización,* Tirant Lo Blanch, Valencia, 2017, p. 305.

[169] *Ibidem*, p. 317.

[170] *Ibidem*, p.319.

[171] *Ibidem*, p. 321.

Bien advierte MUÑOZ CONDE que con las finalidades actuales "se puede convertir en delito de terrorismo, con las graves consecuencias penales que ello conlleva, prácticamente cualquier delito grave que se cometa con intención política. Pero también algunos delitos menos graves, cuando por ejemplo se trata de un daño a un equipo informático, tipificado en el art. 264, como la introducción de virus que altere o haga inaccesibles datos informáticos ajenos si se hace con el fin de desestabilizar el funcionamiento de una institución internacional como el Fondo Monetario Internacional, como protesta por su abusiva política crediticia con los países más pobres…. Los ejemplos de este tipo, pueden multiplicarse dado que algunas de las finalidades mencionada en el art. 573 CP, pueden incluir muchos supuestos que nada tienen que ver con el terrorismo, sino con movimientos sociales de protesta"[172], con lo que en este trabajo hemos denominado hacktivismo. Sería casi equiparar la ya mencionada actividad de Anonymous con el ciberterrorismo, con las consecuencias penológicas, procesales y penitenciarios que ello implica.

En referencia a las penas de prisión, el art. 573 bis CP en su apartado 3, castiga los delitos de terrorismo a los que se refiere el apartado 2, "con la pena superior en grado a la respectivamente prevista en los correspondientes artículos". Es decir, que, para el caso del sabotaje de datos informáticos que alojan infraestructuras críticas para la población, llevadas a cabo con finalidad terrorista, la pena de prisión podría llegar hasta los 7 años y 6 meses. Y en el caso de sabotaje a sistemas de infraestructuras críticas, con finalidad terrorista, se trataría de penas de hasta 12 años de prisión. Sin duda estamos ante conductas graves, siempre que se respete una interpretación estricta tanto de la gravedad del sabotaje como de la finalidad terrorista. Ambas, como hemos visto, se encuentran deficientemente definidas en el código penal, por lo que cabe el riesgo de castigar conductas de sabotaje sin capacidad interruptiva ni destructiva, así como cualquier finalidad política.

9. A modo de conclusiones

Estamos de acuerdo en que, al trasladar nuestros intereses esenciales al ciberespacio, los estados deben repensar y apostar en ciberseguridad. La salud, la energía, el transporte, el agua, la industria, etc., son servicios clave que afectan nuestra vida diaria y dependen cada vez más, de un buen funcionamiento de los sistemas informáticos que contienen las infraestructuras críticas tanto de nuestros países como de la Unión

[172] MUÑOZ CONDE, F., *Derecho penal. Parte Especial, 20º ed. revisada y puesta al día conforme a las leyes orgánicas 1/2015 y 2/2015 de 30 de marzo*, Tirant Lo Blanch, Valencia, 2015, p. 790.

europea. Una realidad reflejada en los datos existentes, ya que, según Europol, "los ataques vienen afectando a una amplia gama de industrias clave e infraestructuras críticas, incluidos los servicios de salud, telecomunicaciones, transporte e industria manufacturera"[173].

Es por eso que la Unión internacional de telecomunicaciones (ITU), que es el organismo de las Naciones Unidas para las tecnologías de la información y comunicación, en su Índice Mundial de ciberseguridad y perfiles de *ciberbienestar (IMC),* al medir el nivel de compromiso de los países con la ciberseguridad contabiliza entre otras cuestiones las medidas jurídicas adoptadas en cada país[174]. Por eso, este trabajo ha versado sobre las medidas jurídicas introducidas en España. Para ello, además de crear diferentes planes y estrategias para la protección de infraestructuras críticas, nuestro país también ha apostado por la introducción de determinados delitos dentro del código penal. Su inclusión, ha obedecido principalmente a la puesta al día de nuestra legislación con los instrumentos internacionales como el Convenio de Budapest, pero también con las Decisiones marco y Directivas europeas en la materia. De esta forma, desde 2010, contamos con dos delitos diferenciados que hacen alusión a la protección tanto del software (datos y programas informáticos) como del hardware (sistemas). En estos instrumentos se pone de manifiesto que lo que se protege es el interés de los operadores y los usuarios de los sistemas informáticos o de telecomunicaciones en su funcionamiento correcto[175]. Sin embrago, la opción que tomó nuestro legislador dista mucho de esta idea, ubicando estas conductas en la rúbrica de los delitos contra el patrimonio y el orden socioeconómico. Una opción que no permite enfocar bien el problema ni recoge los casos más graves que son los que parecen referir los instrumentos internacionales. Entendemos acertado que al trasponer estos instrumentos España aluda a la necesidad de que los daños sean graves, sin embargo, resulta urgente que el legislador defina qué entiende por gravedad, repensando a su vez la posibilidad de manejar otro bien jurídico ante la realidad criminal que se impone. Hemos comprobado cómo la ubicación actual de los delitos no responde a la *ratio essendi* del problema. Según nuestra opinión, lo que es realmente grave, se ha dejado para las agravantes, esto es, que el sabotaje *haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos,* o lo que es más importante*, que el hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad, o que afecten al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la*

[173] *Informe: Evaluación de Amenazas del Crimen organizado en internet,* Europol, 2018, p. 16.

[174] Índice Mundial de ciberseguridad y perfiles de *ciberbienestar (IMC)*, UIT, 2015, p. 1.

[175] Informe Explicativo del Consejo de Europa al Convenio sobre Ciberdelincuencia, (STE, núm. 185) 2001, párrafos 65-70.

Unión Europea o de un Estado Miembro de la Unión Europea. Sin duda, son hechos graves, y que pueden cometerse con una finalidad terrorista, por lo que entendemos que sí deben estar dentro de los delitos de terrorismo, siempre y cuando se acredite no solo la finalidad, sino la gravedad de los hechos.

Finalmente, urge que tanto los gobiernos como la comunidad internacional, dejen de focalizar estos hechos como propios del terrorismo, perfilando también una respuesta jurídica cuando son los propios estados los que llevan a cabo estas conductas. Solo de esta forma estaremos en el camino de conseguir un ciberespacio más libre y más seguro.

Bibliografía

ABOSO, G. E., *La criminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*, BdeF, Buenos Aires, 2017.

ADÁN DEL RÍO, C., "Delitos relativos a los consumidores, delitos informáticos y delitos contra la Hacienda pública", en *Cuadernos penales Jose María Lidón: El anteproyecto de modificación del código penal de 2008. Algunos aspectos,* núm. 6, Universidad de Deusto, 2009.

ALONSO, R., "El terrorismo islamista inspirado en el Islamismo radical", en *Cuadernos de la Guardia Civil, Revista de Seguridad pública*, 3ª época, 2016.

AMBOS, K., "Responsabilidad penal internacional en el ciberespacio", *INDRET: Revista para el análisis del Derecho*, núm. 2, 2015.

ANARTE BORRALLO, E. Y DOVAL PAIS, A. "Límites de la ley penal a propósito del nuevo delito de intrusión informática", en *Revista General de Derecho penal*, núm. 18, 2012.

ANDRÉS DOMÍNGUEZ, A. C., "Los daños informáticos en el Derecho penal europeo", en ÁLVAREZ GARCÍA, F. J., *La adecuación del Derecho penal español al ordenamiento de la Unión Europea. La Política criminal europea,* Tirant Lo Blanch, Valencia, 2009.

ANDRÉS DOMÍNGUEZ, A. C., "Artículo 264 bis", en GÓMEZ TOMILLO, M., *Comentarios prácticos al Código penal, Tomo III, Delitos contra el Patrimonio y socioeconómicos,* Aranzadi, Pamplona, 2015.

ANDRÉS DOMÍNGUEZ, A. C., "Comentario previo a los artículos 264, 264 bis, 264 ter y 264 quater", en GÓMEZ TOMILLO, M., *Comentarios prácticos al Código penal, Tomo III, Delitos contra el Patrimonio y socioeconómicos*, Aranzadi, Pamplona, 2015.

ASÚA BATARRITA, A., "Concepto jurídico de terrorismo y elementos subjetivos de finalidad. Fines políticos últimos y fines de terror instrumental",

en ECHANO BASALDÚA, J. I., *Estudios jurídicos en Memoria de José María Lidón*, Universidad de Deusto, 2002.

BERDUGO GÓMEZ DE LA TORRE, I., "El terrorismo en el s. XXI: del Terrorismo nacional al terrorismo global", en *Revista penal*, núm. 42, 2018.

CANCIO MELIÁ, M., *Los delitos de terrorismo: estructura típica e injusto*, Ed, Reus, Madrid, 2010.

CANO PAÑOS, M. A., "La reforma penal de los delitos de terrorismo en el año 2015. Cinco cuestiones fundamentales", en *Revista General de Derecho penal,* núm. 23, 2015.

CAPITA REMEZAL, M., *Análisis de la legislación penal antiterrorista,* Colex, Madrid, 2008.

CASTRO CORREDOIRA, M. Y VÁZQUEZ-PORTOMEME SEIJAS, F., "La reforma de los delitos de daños: arts. 263, 264, 264 bis, 264 ter, 264 quáter, 265, 266.1, 266.2 CP", en CUSSAC, J. L. (dir.), *Comentarios a la reforma del código penal de 2015, 2ª edición, Actualizada con la corrección de errores (BOE 11 de Junio de 2015)*, Tirant Lo Blanch, Valencia, 2015.

DE LA MATA BARRANCO, N. J., "La tipificación de los denominados daños informáticos", en *Revista de Derecho penal,* núm. 26, 2018.

DE LA MATA BARRANCO, N. J. Y HERNÁNDEZ DÍAZ, L., "El delito de daños informáticos: una tipificación defectuosa", en *Revista de Estudios penales y criminológicos*, vol. XXIX, 2009.

FERNÁNDEZ HERNÁNDEZ, A., "La reforma penal de 2015 en materia de terrorismo: el ocaso de los principios limitadores del Ius Puniendi", en CUERDA ARNAU, M. L. Y GARCÍA AMADO, J.A (dirs.), *Protección Jurídica del Orden Público, la paz pública y la seguridad ciudadana*, Tirant Lo Blanch, Colección delitos, 119, Valencia, 2016.

GARCÍA RIVAS, N., "Delitos de atentado, resistencia y desobediencia", en QUINTERO OLIVARES, G. (dir.), *Comentarios a la Reforma penal de 2015*, Aranzadi, Pamplona, 2015.

GIL GIL, A. Y HERNÁNDEZ BERLINCHES, R. (coords.), *Cibercriminalidad*, Dykinson, Madrid, 2019.

GÓMEZ RIVERO, M. C. (dir.), *Nociones fundamentales de Derecho penal (Vol. II) Parte Especial*, Tecnos, Madrid, 2015.

GONZÁLEZ CUSSAC, J. L., "Servicios de inteligencia y contraterrorismo", en PORTILLA CONTRERAS, G. y PÉREZ CEPEDA, A., *Terrorismo y contraterrorismo en el s. XXI. Un análisis penal y político criminal,* Ratio Legis, Salamanca, 2016.

GONZÁLEZ HURTADO, J. A., "Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: la seguridad en los sistemas de información", en *Revista de Derecho penal, procesal y penitenciario*, núm. 107, 2014.

González Rus, J. J., "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", en *Revista electrónica de Ciencia penal y Criminología*, núm. 1, 1999.

Grupo De Estudios De Política Criminal, "Una alternativa a la actual Política Criminal sobre terrorismo", *Documentos 9*, 2008.

Lamarca Pérez, C., "Análisis de las reformas penales: el caso español", en Serrano-Piedecasas, J. R. y Demetrio Crespo, E. (dirs.); *Terrorismo y Estado de Derecho,* Iustel, Madrid, 2010.

Llobet Anglí, M., "Tema 18. Delitos contra el Orden público", en VV.AA. *Lecciones de Derecho penal. Parte Especial. Cuarta edición adaptada a la LO 1/2015 de reforma del CP*, Atelier, Barcelona, 2015.

Maeztu, D., "Tipificación penal del ransomware", en *Del Derecho y las normas*, 2017. Puede consultarse en https://www.derechoynormas.com/2017/05/tipificacion-penal-del-ramsomware.html (último acceso: 30 de enero 2021).

Mazuelos Coello, J., "Consideraciones sobre el delito de daños informáticos, en especial sobre la difusión de virus informáticos", en *Derecho penal y Criminología: Ejemplar dedicado a Memorias XXIX Jornadas internacionales de Derecho penal. Informática y Derecho penal. Segunda parte*, Vol. 28, núm. 85, 2007.

Merlos García, A., "Internet como instrumento para la Yihad", en *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades*, núm. 16, diciembre 2006.

Miró Llinares, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* Marcial Pons, Madrid, 2012.

Morales Gacía, O., "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas" en Quintero Olivares, G. (dir.), *La Reforma penal de 2010: Análisis y comentarios,* Aranzadi-Thomson, Madrid, 2011.

Morón Lerma, E., "Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos", en *Cuadernos penales José María Lidón: Delito e informática: algunos aspectos*, núm. 4, Universidad de Deusto, Bilbao, 2007.

Muñoz Conde, F., *Derecho penal. Parte Especial, 20º ed. revisada y puesta al día conforme a las leyes orgánicas 1/2015 y 2/2015 de 30 de marzo*, Tirant Lo Blanch, Valencia, 2015.

Navarro Cardoso, F., "El delito de financiación del terrorismo en el código penal español (art. 576 CP)", en Ferré Olivé J. C. y Pérez Cepeda, A. I. (dirs.); *Financiación del Terrorismo,* Tirant Lo Blanch, Valencia, 2018.

Ortigosa, A., "Las nuevas amenazas cibernéticas del s. XXI. Ciberterrosrimo: nueva forma de subversión y desestabilización", en *Cuadernos de la Guardia Civil. Revista de Seguridad públic*a, 3ª época, 2016.

PÉREZ CABALLERO, J., "Defensa de los elementos contextual y político de los crímenes de lesa humanidad contra la expansión del tipo al terrorismo internacional", en *Revista electrónica de Ciencia penal y Criminología, núm.15,* 2013.

PÉREZ CEPEDA, A. I., *El Pacto antiyihadista: criminalización de la radicalización,* Tirant Lo Blanch, Valencia, 2017.

PÉREZ-PRAT DURBÁN, L., "Los ciberataques y el uso de la fuerza en las relaciones internacionales", en MILLÁN MORO, L. (dir.), *Ciberataques y ciberseguridad en la escena internacional,* Aranzadi, Pamplona, 2019.

ROBLES PLANAS, R. Y PASTOR MUÑOZ, N., "Tema 12: Delitos contra el patrimonio (III)", en VVAA, *Lecciones de Derecho Penal, Parte especial, Cuarta edición adaptada a la LO 1/2015 de reforma del CP*, Atelier, Barcelona, 2015.

ROMEO CASABONA, C. M., "Los delitos de daños en el ámbito informático", en *Cuadernos de Política criminal,* n*úm. 43,* 1991, p. 92.

RUÍZ DÍAZ, J., "Ciberamenazas, ¿el terrorismo del futuro?", en *Boletín IEEE*, núm. 3, Julio-Septiembre, 2016.

SALVADORI, A., "Los nuevos delitos informáticos introducidos en el código penal español con la Ley Orgánica 5/2010", en PÉREZ ÁLVAREZ, F., *Delito, pena, política criminal y tecnologías de la información y la comunicación en las modernas Ciencias penales*, Ediciones Universidad de Salamanca, 2012.

SORIANO, M., "Seguridad en redes y seguridad de la información", *Improvet: Proyecto financiado por la Comisión Europea,* Publicado por České vysoké učení technické v Praze. *C*onsultar en https://docplayer.es/4814747-Seguridad-en-redes-y-seguridad-de-la-informacion-miguel-soriano.html (Último acceso 16 de septiembre de 2020).

TORRES SORIANO, M. R., "El hacktivismo como estrategia de comunicación. De Anonymous al Cibercalifato", en *Cuadernos de Estrategia,* núm. 197, 2018.

VALVERDE, L., "Estamos perdiendo la ciberguerra: Estados Unidos lleva tiempo usando la tecnología digital para atacar a sus enemigos", en *EL País* de 16 de Julio de 2013. Consultar en http://elpais.com/elpais/2013/07/12/opinion/1373622319_413845.html (último acceso: 15 de septiembre de 2020).

VILLALBA FERNÁNDEZ, A. Y CORCHADO RODRÍGUEZ, J. M., "Análisis de las ciberamenazas", en *Cuadernos de estrategia*, núm. 185, 2017.