LA FIGURA DEL CENTINELA INFORMÁTICO EN EL NUEVO CÓDIGO PENAL MILITAR COMO SUJETO PASIVO Y ACTIVO DE DELITOS: CAPACIDADES DE ACTUACIÓN, DEBERES Y VULNERABILIDADES

Premios de Defensa 2018

Modalidad Premio José Francisco Querol y Lombardero

SUMARIO

1. INTRODUCCIÓN

En los últimos cincuenta años, el avance tecnológico producido en las sociedades contemporáneas ha sido prácticamente inconmensurable. Desde los teléfonos móviles, pasando por la *world wide web*, los sistemas SCADA, los drones y un largo etcétera, las posibilidades para el desarrollo, la comunicación, la generación de riqueza y la simplificación de procesos se han multiplicado exponencialmente.

La multiplicidad de capacidades y oportunidades se ha traducido también en una ampliación de las modalidades de comisión de conductas que, en ocasiones, cumplen los parámetros del delito. A veces, las nuevas herramientas simplemente han abierto otros caminos por los que cometer antiguos y conocidos crímenes, lo que ha dificultado, además, su averiguación y persecución. En otras ocasiones, estos avances han generado

nuevos tipos delictivos, al construirse una nueva realidad con sus capas física, digital y social, que deben ser protegidas[1]. En todo caso, este avance tecnológico constante y vertiginoso presenta unas características o perfiles que llevan al surgimiento de nuevas vulnerabilidades de bienes jurídicos necesitados de protección, como es el caso de la seguridad y defensa nacional. Así, por ejemplo, Romeo Casabona[2] resume los perfiles del avance tecnológico que llevan a un incremento de las vulnerabilidades de los bienes jurídicos en tres puntos:

1. La capacidad para procesar, albergar y circular, de forma automatizada y en tiempo real, ingentes cantidades de información digital. La estructura descentralizada y no jerarquizada de las redes es incompatible con la existencia de órganos de control de dicha información o la posibilidad de establecer censuras o supervisiones.
2. El colosal número de usuarios, con multiplicidad de plataformas de acceso, desde cualquier punto geográfico, conjugado con la libertad para emitir, transferir y difundir información de forma anónima o seudoanónima.
3. Las características físicas y técnicas de las propias tecnologías y sistemas, que permiten su intervención o alteración con los más variados métodos sin autorización o consentimiento.

Por su parte, Rovira del Canto habla de similares aspectos de la evolución tecnológica[3]: la facilidad en el acceso, búsqueda, intercambio y difusión de información, la globalización del fenómeno y la existencia de un espacio virtual, el ciberespacio, en el que «los delitos no solo pueden ser cometidos por cualquiera, sino que también amenazan a cualquier ciudadano». A ello añade acertadamente Miró Llinares los caracteres de, primero,

---

[1] Se entiende por *capa física* el conjunto de elementos reales, la infraestructura, sobre la que se sustenta la tecnología, por ejemplo, satélites, cables y puntos de Internet (IXP, *Internet exchange points*); la capa digital está conformada por los elementos digitales y telemáticos, los protocolos de Internet, los nombres de dominio, las direcciones digitales; finalmente, la capa social está configurada por los propios usuarios, así como por elementos reguladores de los sistemas. Del mismo modo, la seguridad debe construirse sobre esas tres capas, con restricciones de acceso a las infraestructuras físicas, con el desarrollo de sistemas de seguridad informáticodigitales y con el desarrollo de sistemas de educación y concienciación de uso seguro y herramientas de protección simple para los usuarios.

[2] ROMEO CASABONA, C. M. (coord.). *El Cibercrimen: nuevos retos jurídicopenales, nuevas respuestas político-criminales*. Madrid: Comares 2006, pág. 3.

[3] ROVIRA DEL CANTO, E. «Las nuevas pruebas telemática y digitales. Especialidad de la prueba en delitos cometidos por Internet». *Jornadas sobre la prueba en el Proceso Penal. Estudios Jurídicos, Ministerio Fiscal*, vol. I. Madrid: CEJAJ 2003.

neutralidad de la Red, en el sentido de que en su actual configuración, una vez existe el acceso a Internet, ni siquiera el propio operador puede impedir el acceso a una web elegida por el usuario, y, segundo, de permanente evolución tecnológica de las TIC (tecnologías de la información y la comunicación) en general y del ciberespacio en particular; destaca la aparición de nuevos servicios y la continua ampliación y modificación de formas de acceso, lo que conlleva la temporalidad de la eficacia de las posibles barreras de protección[4].

Estos perfiles y caracteres generan, al margen del abordaje criminológico doctrinal y normativo que se haga de la materia[5], unas circunstancias de comisión delictiva que suman, como venimos señalando, nuevos problemas y vulnerabilidades[6], así, en primer lugar, y como hemos apuntado, la dificultad de determinar el ámbito geográfico tanto en relación con el origen (sujeto activo) como con el destino (sujeto pasivo u objeto); la facilidad de la comisión delictiva debido a los pocos recursos necesarios para dicha actividad delincuencial y, en muchos tipos penales, sin necesidad de conocimientos específicos sobre informática; las múltiples jurisdicciones[7];

---

[4] MIRÓ LLINARES, F. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons, pp. 143-160.

[5] Existen diversos abordajes tanto doctrinales como normativos en relación con el fenómeno de la ciberdelincuencia, desde quienes hablan de *delitos informáticos*, limitando la definición a aquellos crímenes en los que la tecnología es lo que aporta la particularidad de estos, hasta aquellos que prefieren hablar de una categoría criminológica de *cibercrimen*, donde se englobarían también delitos tradicionales cometidos a través de la Red (amenazas, etc.) o en los que la tecnología es un mero apoyo (contratación de un asesino a sueldo en la *Deep Web*). Del mismo modo, la sistematización penal varía y existen diferentes opiniones sobre cómo este tipo de delitos debería integrarse y tipificarse en los textos penales. *Vid*., entre otros, MIRÓ LLINARES, F. *Op. cit.*; JEWKES, Y. y YAR, M. (eds.). *Handbook of Internet Crime*. Devon: William Publishing 2010; CLIMENT BARBERÁ, J. «La justicia penal en Internet. Territorialidad y competencias penales». *Cuadernos de derecho judicial*, n.º 10. Madrid: 2001; Convenio sobre Ciberdelincuencia de 23 de noviembre de 2001 del Consejo de Europa; Instrucción 2/2011 de la Fiscalía General del Estado sobre el Fiscal de Sala de Criminalidad Informática de las Fiscalías, de 11 de octubre de 2011.

[6] DÍAZ GÓMEZ, A. «El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest**».** *REDUR,* n.º 8, diciembre 2010, p**ág**. 173.

[7] El caso Yahoo*:* en aplicación del principio de territorialidad, el Tribunal de Gran Instancia de París condenó a la empresa Yahoo por la venta en territorio francés de artículos de orientación nacionalsocialista (art. 645.1 CP francés). El Alto Tribunal impuso a la mencionada empresa la obligación de destrucción de todos los datos, el bloqueo a los usuarios franceses a la página web y la prohibición de venta de los susodichos artículos. Hasta aquí no existe objeción alguna; el problema era que la empresa Yahoo tenía (y tiene) su sede en territorio estadounidense, y alegó que la orden era imposible de cumplir. Ello porque en EE. UU. la venta de productos relacionados con el nacionalsocialismo no es delito alguno y los servidores de la empresa se hallaban en dicho país. Igualmente, también se consigue demostrar la dificultad para identificar con seguridad los usuarios franceses que accedían a

la transnacionalidad; la continuidad delictual vinculada al automatismo del hecho; extensa y elevada lesividad[8]; el problema de la responsabilidad penal, tanto desde el punto de vista de las posibilidades de anonimato como el de la responsabilidad de las personas jurídicas[9], y, por supuesto, la búsqueda y aportación de pruebas válidas para el inicio y la tramitación de cualquier proceso penal.

Todo lo anteriormente apuntado obliga a una adaptación de las normativas penales y procesales de los Estados a fin de enfrentar adecuadamente el fenómeno delincuencial asociado a dicho componente tecnológico. Esa adaptación debe partir de un análisis específico tanto de las capacidades como de los riesgos que ofrece la tecnología para articular tanto una protección ajustada y realista de los bienes jurídicos como métodos de investigación criminal apropiados, lo que exige tener en cuenta la rapidez de la evolución tecnológica y la necesidad de flexibilidad y coordinación nacional e internacional a la hora de enfrentar esta delincuencia y sus diversas manifestaciones. Forma parte de ello la adaptación de la normativa penal y procesal militar, más teniendo en cuenta que el bien jurídico seguridad y defensa nacional se revela como uno de los más vulnerables a las capacidades tecnológicas de sujetos, grupos y Estados.

En este sentido, el nuevo Código Penal Militar (CPM), aprobado por Ley Orgánica 14/2015 de 14 de octubre, ha introducido algunas novedades en relación con dicha materia. Esta llamémosla *dimensión tecnológica* va más allá de la inclusión de los denominados genéricamente delitos de daños informáticos[10], y se revela como de gran importancia la nueva figura del que podríamos denominar *centinela informático*, una figura, a nuestro entender, fundamental a la hora de analizar la conexión entre tecnología y protección de los bienes jurídicos militares, debido a sus capacidades de actuación, sus deberes y sus vulnerabilidades.

---

la página web en cuestión. Esta constituye una demostración palpable de los problemas aludidos, incluso plantea la cuestión respecto de que un país tenga o no el derecho de imponer sus leyes a compañías de otro país.

[8] DE LA CUESTA ARZAMENDI, J. J.; PÉREZ MACHÍO, A. U.; SAN JUAN GUILLÉN, C. «Aproximaciones criminológicas a la realidad de los ciberdelitos». DE LA CUESTA ARZAMENDI, J. J. (Dir.). *Derecho penal informático*. Madrid: Cívitas 2010, pp. 85-87.

[9] *Vid*. GÓMEZ TOMILLO, M. *Responsabilidad penal y civil de los delitos cometidos a través de Internet*. Cizur: Aranzadi 2004; y MORALES GARCÍA, O. «Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (artículo 197 3 y 8, 264 y 258)». QUINTERO OLIVARES, G. *La reforma penal de 2010: Análisis y comentarios*. Cizur: Aranzadi 2010.

[10] Artículos 264 a 266 del Código Penal, a los que remite el artículo 27 del Código Penal Militar.

2. EL CENTINELA INFORMÁTICO EN EL NUEVO CPM

La figura de centinela se remonta a los inicios de formación de cualquier grupo armado, ya fuese temporal o permanente, toda vez que su función principal, la vigilancia y resguardo de un lugar asignado, se evidencia como esencial para la seguridad de dichos grupos y sus apoyos, sean estos enseres, transportes, instalaciones, etc.

Ello conlleva que la protección especial que se le dispensa en los sucesivos códigos penales militares dimane de la protección del bien jurídico seguridad y defensa nacional, y no del de la vida o la integridad física, sin perjuicio de que estos también puedan resultar dañados en un ataque a dicha figura. Del mismo modo, la esencialidad de la función del centinela lleva a la tipificación de delitos que pueden ser cometidos de forma específica por este al afectar negativamente al desempeño correcto de esta, como analizaremos más detenidamente.

Pero ¿qué es, desde el punto de vista penal, un centinela?

En el Código Penal Militar de 1985, el artículo 11 definía esta figura de la siguiente manera:

> «Es centinela el militar que, en acto de servicio de armas y cumpliendo una consigna guarda un puesto confiado a su responsabilidad.
>
> Tienen además dicha consideración los militares que sean: componentes de las patrullas de las guardias de seguridad en el ejercicio de su cometido; operadores de las redes militares de transmisiones o comunicaciones durante el desempeño de sus funciones; operadores de sistemas electrónicos de vigilancia y control de los espacios terrestres, marítimos y aéreos confiados a los centros o estaciones en que sirven, durante el desempeño de sus cometidos u observadores visuales de los mismos espacios»[11].

Esta aparentemente sencilla definición no ha estado exenta de disputa jurisprudencial, toda vez que la correcta atribución de dicha cualidad al

[11] Como complemento a esta definición, y sin diferir sustancialmente en el contenido, encontramos el artículo 24 del Real Decreto 194/2010, de 26 de febrero, por el que se aprueban las Normas sobre Seguridad en las Fuerzas Armadas:

«1. Son centinelas los componentes de la guardia de seguridad que, en acto de servicio de armas y cumpliendo una consigna, guardan un puesto confiado a su responsabilidad portando a la vista el arma de fuego que por su cometido les corresponda.

2. El centinela se empleará para la defensa y protección de lugares o instalaciones sensibles donde el grado de seguridad lo exija y su utilización será restrictiva.

3. Tienen además la consideración de centinela aquellos que, por la importancia o trascendencia de las funciones o cometidos que desempeñen, así les sea reconocida por la legislación vigente».

sujeto resulta imprescindible para la definición de los elementos del tipo penal, tanto cuando el centinela es sujeto pasivo como cuando es sujeto activo del delito. Así, la Sentencia de la Sala Quinta del Tribunal Supremo de 23 de enero de 2013 (STS 496/2013) señala:

> «A propósito de la figura del centinela, hemos declarado con reiterada virtualidad que su concepto legal a efectos penales es el que se contiene en el art. 11 CPM, precepto en que incluye tanto a quien lo es en sentido estricto, es decir, "el militar que, en acto de servicio de armas y cumpliendo una consigna, guarda un puesto confiado a su responsabilidad", como a quienes también reúnen esta consideración por asimilación legal comprensiva de quienes "sean componentes de las patrullas de las guardias de seguridad en el ejercicio de su cometido", por lo que la condición de centinela hemos dicho que es cuestión jurídica, ante todo (Sentencias 16.03.1998, 25.11.2002 y 22.03.2004). Y asimismo hemos sostenido con igual reiteración que el bien jurídico que la norma protege radica en la especial relevancia de las funciones que el centinela tiene encomendadas en el desempeño de su misión, de velar por la seguridad de las Fuerzas Armadas y de sus instalaciones así como por el normal desenvolvimiento de las funciones militares, a lo que se añade la integridad física de las personas que las realizan cuando se trata de la modalidad de maltrato de obra; lo que justifica la especial y reforzada protección penal que se otorga a dicho sujeto (*vid*. nuestra reciente Sentencia 29/11/2011 y las que en ella se citan)».

En todo caso, vemos que en el concepto legal a efectos penales se incluyen tanto los operadores de redes de transmisiones y comunicaciones como de sistemas electrónicos de vigilancia y control, lo que evidencia la relevancia de la vulneración de redes de trasmisiones, comunicaciones y sistemas electrónicos para la seguridad nacional[12].

Recogiendo los avances tecnológicos a los que nos hemos referido y su penetración especialmente destacable en el ámbito militar, el nuevo Código Penal Militar recoge también en el concepto legal de centinela, ahora establecido en el artículo 4[13], a los *operadores de redes informáticas*. Ello

[12] El Código de Justicia Militar de 1945 ya recogía en su artículo 358 el abandono del servicio de transmisiones y su relevancia para la defensa nacional.

[13] Artículo 4:

«1. Es centinela, a los efectos de este Código, el militar que, en acto de servicio de armas y cumpliendo una consigna, guarda un puesto confiado a su responsabilidad, portando a la vista el arma de fuego que por su cometido le corresponda.

2. Tienen además dicha consideración los militares que sean:

a) componentes de las guardias de seguridad en el ejercicio de su cometido;

añade una específica complejidad a los delitos vinculados a esta figura que vamos a tratar de analizar a lo largo de las siguientes páginas.

Dado que el concepto legal de *centinelaoperador de redes informáticas militares* se produce por asimilación legal, su configuración como tal no depende del cumplimiento de los requisitos establecidos en el apartado 1, esto es, de que sea un militar que «en acto de servicio de armas y cumpliendo una consigna guarda un puesto confiado a su responsabilidad, portando a la vista el arma de fuego que por su cometido le corresponda». Por tanto, lo que nosotros hemos venido en denominar *centinela informático* no precisa portar a la vista ningún arma de fuego, del mismo modo que no es preceptivo en el caso del resto de los operadores de redes y sistemas.

La cuestión central que determinar, tanto en el caso de su configuración como sujeto pasivo como en el de sujeto activo de los tipos penales vinculados a dicha figura, es qué es un operador de redes informáticas; hay que delimitar, por tanto, el concepto de centinela en el ámbito real del desempeño de estos cometidos.

Así, si acudimos al significado del término en el ámbito civil, los operadores de redes informáticas son los sujetos encargados de gestionar las infraestructuras de informática y tecnología de una empresa, en este caso, de las Fuerzas Armadas. Ello implica la gestión tanto de los diferentes elementos físicos de la red (*switches, routers*, *access point*, etc.) como la gestión de la capa *software* que permita un correcto funcionamiento del flujo de datos y segurización en el acceso a la infraestructura (por ejemplo, habilitando o deshabilitando el acceso en función del perfil de usuario, gestionando la clave de acceso wifi, evaluando que los tiempos de latencia en las comunicaciones son correctos, etc.). Entre sus funciones estarían:

- Configuración y administración de la infraestructura, donde destacan:
  - Red LAN[14]
  - Red WAN[15] (wide area network o red de área amplia).

b) operadores de las redes militares de transmisiones, comunicaciones o informáticas durante el desempeño de sus cometidos; y

c) operadores de sistemas electrónicos de vigilancia y control de los espacios confiados a los centros o estaciones en que sirven u observadores visuales de los mismos espacios, durante el desempeño de sus cometidos».

[14] Red interconectada en un área reducida. En el ámbito del Ministerio de Defensa se denomina LAN PG: redes de área local de propósito general.

[15] Red que permite conectar múltiples dispositivos ubicados en diversas redes (LAN) e interconectadas entre sí aunque estén ubicados a grandes distancias; por ejemplo, una empresa que pueda tener varias delegaciones en todo el mundo y que estas estén conectadas

- − Red telefonía
- − Red wifi
- − Elementos de seguridad
- − Elementos de infraestructura física

• Atención e interlocución para incidencias de la infraestructura realizando diagnóstico inicial.

Monitorización y primer diagnóstico de las incidencias surgidas en la red.

En el ámbito del Ministerio de Defensa y de las Fuerzas Armadas, la seguridad de los sistemas y tecnologías de la información se desarrolla a partir de una normativa de primer, segundo y tercer nivel[16], que lleva a la existencia de diverso personal que desarrolla tareas vinculadas a las TIC en las diferentes unidades militares y en el propio Ministerio de Defensa y, por tanto, a la existencia de múltiples sujetos que, en determinado momento, podrían estar cumpliendo las funciones de operador de red de transmisión y comunicación y, de forma acumulada o independiente, de redes informáticas.

Pero debemos destacar que en el marco de las Fuerzas Armadas existe un mando operacional específicamente destinado a una función genérica de vigilancia y salvaguarda de la defensa nacional en el ámbito del ciberespacio. Hablamos del Mando Conjunto de Ciberdefensa (MCCD), creado por Orden Ministerial 10/2013, de 19 de febrero, y actualmente regulado por la Instrucción 65/2015, de 30 de diciembre, del jefe de Estado Mayor de la Defensa, por la que se desarrolla la Organización del Estado Mayor

---

entre sí. En el ámbito del Ministerio de Defensa se denomina Red de Área Extensa Propósito General del Ministerio de Defensa (WAN PG).

[16] *Vid*. especialmente el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica; el Plan Director de Sistemas de Información y Telecomunicaciones, aprobado por la Orden DEF/315/2002; la Orden DEF/2639/2015 sobre Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del MINISDEF; la Instrucción 53/2016, de 24 de agosto, del secretario de Estado de Defensa, por la que se aprueban las Normas para la Aplicación de la Política de Seguridad de la Información del Ministerio de Defensa*;* la Instrucción 58/2016, de 28 de octubre, del secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa; el Procedimiento de Gestión de Incidencias TIC y la Instrucción 345-seginfo/01/12/v1 sobre Política de Seguridad de las Redes de Área Local de la WAN PG del Ministerio de Defensa.

En todo caso, de forma más genérica tampoco debe olvidarse que, dadas las características del ciberespacio, la estrategia de ciberseguridad es global, con la importante colaboración entre el CERT (Computer Emergency Response Team) del Centro Criptológico Nacional, el del INCIBE (Industria) y el del propio MCCD, entre otros, en el marco de la Estrategia Nacional de Ciberseguridad (2013), la cual puede consultarse en https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf.

de la Defensa. El Mando Conjunto de Ciberdefensa tiene la estructura y funciones establecidas en el artículo 15 del Real Decreto 872/2014, de 10 de octubre, en el artículo 11 de la Orden DEF/166/2015, de 21 de enero, y en el artículo 3 de la Orden DEF/1887/2015, de 16 de septiembre.

Concretamente el MCCD es «la unidad encargada del planeamiento y ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del MINISDEF u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional».

No todo el personal destinado en el MCCD lleva a cabo las mismas funciones. En su estructura se ha establecido un Estado Mayor, que cuenta, entre otras, con una Sección de Ciberinteligencia y Seguridad y otra de Operaciones; El mando cuenta además con una jefatura específica de operaciones, «responsable de la ejecución de operaciones de ciberdefensa a través de las acciones de defensa, explotación y respuesta en el ciberespacio, coordinando técnicamente las actividades de los centros de operaciones de seguridad del MINISDEF, tanto permanentes como desplegables».

Dadas estas funciones específicas asignadas, podemos encontrar un gran número de militares en funciones de centinela informático en dicho ámbito. Además, no solo los militares destinados en dicho mando pueden ser considerados como tal en exclusiva, al existir, como hemos señalado, unidades en la estructura de los Ejércitos y la Armada con competencias sobre la materia, así como centros de seguridad (COS) tanto permanentes como desplegables. Ahora bien, partiendo del concepto legal contenido en el artículo 4, será necesario acreditar, en cada caso concreto, que nos encontramos ante un militar desempeñando la función de *operador de redes informáticas* en el ámbito de las Fuerzas Armadas para poder considerarlo centinela a los efectos oportunos.

En este sentido, ya en la Orden Ministerial 50/2011, de 28 de julio, por la que se aprueban las Normas sobre Mando y R*égimen* Interior de las Unidades e Instalaciones del Ejército de Tierra[17], se hablaba específicamente de las guardias de servicio de los sistemas CIS; el artículo 98.4 señala:

[17] La Orden Ministerial 12/2012, de 28 de febrero, por la que se aprueban las Normas sobre Mando y R*égimen* Interior de las Unidades de la Armada, y la Orden Ministerial 50/2011, de 28 de julio, por la que se aprueban las Normas sobre Mando y R*égimen* Interior de las Unidades e Instalaciones del Ejército de Tierra. La Orden Ministerial 13/2012, de 28 de febrero, por la que se aprueban las Normas sobre Mando y R*égimen* Interior de las Unidades del Ejército del Aire no hacen referencias específicas a la figura del centinela, y se remiten en todo caso al RD 194/2010 antes citado de Seguridad de las FAS.

«Las guardias del servicio de los sistemas CIS se regirán por lo establecido en estas normas, por las que se establezcan con carácter general y por las específicas del servicio. A efectos de aplicación de la legislación penal militar, los operadores de este servicio tienen la consideración de centinela».

Delimitado, por tanto, el concepto del sujeto, vamos a pasar a analizar en las siguientes páginas la relevancia penal específica de dicha figura.

2.1. El centinela informático como sujeto pasivo de delitos

Dada, como señalábamos, la relevancia de la figura del centinela para la protección del bien jurídico seguridad y defensa nacional, su amparo se ha venido recogiendo tradicionalmente en los textos penales militares. En la actualidad, el CPM de 2015 regula dicha protección en su artículo 34:

«El que desobedeciere o hiciere resistencia a órdenes de centinela será castigado con la pena de tres meses y un día a dos años de prisión. Si le maltratare de obra será castigado con la pena de cuatro meses a tres años de prisión, sin perjuicio de la pena que pueda corresponder por los resultados lesivos producidos conforme al Código Penal.

Se impondrán las penas superiores en grado a las respectivamente señaladas en el párrafo anterior cuando concurra alguna de las circunstancias siguientes:

1. Si el hecho se verifica con armas u otro medio peligroso.
2. Si la acción se ejecuta en situación de conflicto armado, estado de sitio o en el curso de una operación internacional coercitiva o de paz».

El tipo penal es, en su modalidad de maltrato de obra, claramente pluriofensivo, como se ha reiterado por numerosa jurisprudencia de la Sala Quinta del TS[18], de tal forma que la vida e integridad física del sujeto pasivo también quedan protegidas. En los casos de centinelas tradicionales, es decir, aquellos comprendidos en el número 1 del artículo 4 del CPM, y al margen de las mayores o menores dificultades probatorias de un suceso

[18] «El bien jurídico que la norma protege, hemos dicho que radica en la especial relevancia de las funciones que el centinela tiene encomendadas en el desempeño de su misión, de velar por la seguridad de las Fuerzas Armadas y de sus instalaciones, así como por el normal desenvolvimiento de las funciones militares, a lo que se añade la integridad física de las personas que las realizan cuando se trata de la modalidad de maltrato de obra; lo que justifica la especial y reforzada protección que se otorga a dicho sujeto». STS n.º 1824/2013 de 16 de abril. *Vid*. también sentencias 23.01.1992, 14.02.1994, 08.05.1995, 16.03.1998, 07.11.2001, 25.11.2002, 03.03.2003 y 08.04.2005.

concreto, resulta más o menos fácil imaginar un hecho típico de desobediencia directa a una orden de un centinela, como puede ser traspasar la entrada de una instalación militar contraviniendo la prohibición del centinela o una agresión con un arma, etc.

Más difícil resulta intentar delimitar qué conductas podrían ser subsumidas en este tipo penal cuando el sujeto pasivo es el operador de redes informáticas.

En primer lugar, indudablemente también podría ser posible que fuese objeto del maltrato de obra, con el objetivo, por ejemplo, de acceder al terminal informático que dicho centinela esté manejando en un determinado momento. Sin embargo, esta modalidad no presenta ninguna diferencia o novedad en el análisis penal con el maltrato a un *centinela de puerta*, y por tanto no vamos a detenernos en ello.

Lo que cabe plantearse teniendo en cuenta el entorno cibernético en el que el centinela informático desempeña sus cometidos, cuya relevancia es precisamente lo que da lugar a la consideración penal de un operador de redes informáticas como centinela, es si el empleo de herramientas informáticas o tecnológicas para contravenir sus configuraciones de seguridad informática podrían cumplir con los elementos del tipo en su modalidad de desobediencia o resistencia a órdenes.

Los principios de legalidad y tipicidad nos obligan a limitar la interpretación extensiva y analógica en este sentido. Así, la primera dificultad parte de la definición legal de *orden*, también contenida en el Código Penal Militar en su artículo 8 (antiguo 19): «Es orden todo mandato relativo al servicio que un superior militar da a un subordinado, en forma adecuada y dentro de las atribuciones que le corresponden, para que lleve a cabo u omita una actuación concreta».

Ahora bien, la jurisprudencia de la Sala Quinta del TS es clara al desvincular los mandatos del centinela del concepto de orden contenido en el artículo 8 del CPM. Así:

> «De la anterior condición funcional y del ajuste a los cometidos que al centinela se asignan resulta la legitimidad de su actuación en cuanto a las órdenes que este emite, que, lógicamente, no pueden sino obedecer a causas que conecten con el cumplimiento de la consigna que aquel hubiera recibido. El módulo inmediatamente aplicable al afecto no es el que se establece en el art. 19 CPM, que está previsto para los mandatos que un militar superior da a otro subordinado en relación con el servicio para que este último se comporte en determinado sentido. Quien ostenta la condición de centinela emite requerimientos

> o mandatos imperativos en el cumplimiento de la misión de seguridad que cumple que no se identifican con las órdenes en sentido estricto a que se refiere el art. 19 CPM., porque el destinatario de aquellos puede ser cualquier persona militar o civil y aún en el primer supuesto, como es el caso que se examina, no es necesario que el militar se encuentre en el desempeño de un acto propio del servicio ni ser subordinado de quien imparte la orden. Por ello, además, la desobediencia genérica se encuentra tipificada en el art. 102 CPM., mientras que esta tiene carácter específico y se contrae a la conducta desobediente respecto de los mandatos que emite un centinela en el desempeño legítimo de su misión»[19].

Es el caso de un centinela de puerta, por ejemplo, que ordena retirar un vehículo de una zona de seguridad fuera de la instalación militar, y el conductor se niega a realizarlo, «frustrando así la salvaguardia de la seguridad de las instalaciones militares que, cumpliendo su misión, pretendía el centinela al requerirle para que retirase el vehículo, por lo que la alegación de la parte fundamentada en el corto retraso en el cumplimiento de lo ordenado —ya que una vez realizada su actividad retiró la furgoneta— resulta irrelevante porque ese retraso era suficiente para la ineficacia de la protección del interés militar que subyacía en la orden»[20].

Por tanto la cuestión sería: ¿Pueden considerarse órdenes las actividades desarrolladas por los operadores de redes informáticas en sus funciones de monitorización y defensa de las redes y sistemas? Parece difícil que la función genérica de un operador de red pueda ser interpretada como una orden; en nuestra opinión supondría una interpretación extensiva que vulneraría el principio de legalidad. Planteemos entonces la siguiente situación:

Un sujeto (militar o paisano) accede sin autorización a una de las redes o sistemas de las FAS. En su función de centinela, un militar detecta dicha intrusión y no solo lleva a cabo las necesarias acciones informáticas defensivas, sino que interactúa con el atacante en el ámbito virtual para darle instrucciones específicas que lleven a poner fin a esa conducta. ¿Esas interacciones o instrucciones pueden ser consideradas órdenes de un centinela? Parece que dichas instrucciones sí podrían ser incardinadas en los «requerimientos o mandatos imperativos que el centinela emite en el cumplimiento de la misión de seguridad que cumple».

[19] STS de la Sala Quinta n.º 7311/2007, de 5 de noviembre.
[20] STS de la Sala Quinta n.º 7825/2002, de 25 de noviembre.

La cuestión cobra relevancia cuando la conducta en sí resulta atípica según otros tipos del Código Penal. Así, el mero acceso no consentido *(hacking)*[21] no se contempla como delito en el CPM, ni por remisión al Código Penal ordinario[22], por tanto cabría plantearse que, si se ha puesto en peligro el bien jurídico seguridad y defensa nacional a través de ese acceso y mantenimiento en el sistema, en el que específicamente se han desobedecido las instrucciones dadas por el centinela informático, o contravenido su voluntad, podríamos encontrarnos ante el artículo 34 del CPM, y no ante el artículo 197 bis 1 del Código Penal ordinario[23].

Para resolverlo, vamos a analizar dicho artículo del CP común, que tipifica el *hacking* de la siguiente manera:

> «El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad

---

[21] El *hacking* es el acceso ilícito a los sistemas informáticos. La base de la ilicitud es la falta de conocimiento y consentimiento del titular, y no el resultado del acceso, que puede o no conllevar daños, alteraciones o uso de los datos, y es lo que lleva a diferenciar, en el ámbito técnico, a los *hackers* blancos de los grises/negros *(crakers)*. En todo caso, el *hacking* implica siempre un acceso remoto (no el uso del terminal físico del titular) y supone la entrada en el sistema, atravesando las barreras de protección que puedan existir o usando *puertas* que puedan estar abiertas. La extracción de datos a través de *malware* sin que de hecho se produzca un acceso sería otra modalidad delictiva, que no implicaría *hacking*.

[22] Algunos autores sostienen que «el acceso no autorizado inevitablemente va a suponer algún tipo de alteración de los datos del mismo porque la sola entrada y uso del sistema da lugar a la modificación de los datos, a lo que hay que añadir que con frecuencia los *hackers* realizan alteraciones en dichos datos para intentar borrar los rastros que puedan identificarles». RODRÍGUEZ, G.; ALONSO, J.; LASCURAÍN, J. A. «Derecho penal e Internet». FERNÁNDEZ ORDÓÑEZ, M.; CREMADES GARCÍA, J.; ILLESCAS ORTIZ, R. (coords.). *Régimen Jurídico de Internet*. Madrid: Wolters Kluver 2001, pág. 269. En caso de que efectivamente se produzcan acciones de alteración de datos que cumplan con los requisitos del delito de daños del artículo 264 del CP ordinario, al que sí remite el CPM —y que analizaremos con detenimiento en páginas posteriores—, nos encontraríamos en dicho ámbito. Consideramos que el artículo 197 describe una conducta diferente en la que las posibles modificaciones de datos son mínimas e irrelevantes y existen además bienes jurídicos diferentes bajo protección. Como señala Morales García, se trata de una conducta que «supone un adelantamiento de la barrera que separa la intervención penal de otro tipo de intervenciones jurídicas, puesto que la integridad de los sistemas ya es objeto de tutela a través de los delitos de daños informáticos e interferencia de sistemas». MORALES GARCÍA, O. «Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (artículo 197 3 y 8, 264 y 258)». QUINTERO OLIVARES, G. *La reforma penal de 2010: Análisis y comentarios*. Madrid: Aranzadi 2010, pág. 184.

[23] Introducido por Ley 5/2010 de 22 de junio, en aplicación de la Decisión Marco 2005-222-JAI, como artículo 197.3, si bien también se encuentra recogido en el Convenio de Budapest.

de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años».

Vamos a examinar brevemente los elementos de este tipo delictivo, centrándonos en una cuestión que para nosotros se evidencia especialmente relevante para abordar la posible tipificación de la conducta a la que hacíamos referencia como un delito del artículo 34 del CPM, y no de este artículo 197 bis 1 del CP común; dicha cuestión es la relativa al bien jurídico que se tutela con este último, si bien la ubicación del tipo 197 bis 1 en el capítulo I «Del descubrimiento y revelación de secretos» del título X «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio» podría llevarnos a afirmar sin más reflexión al respecto que se trata de un delito contra la intimidad personal, la cuestión no está ni mucho menos exenta de polémica. Como resume Colás Turégano[24], la doctrina mayoritaria[25] se ha decantado por sostener que lo que se pretende proteger con esta figura es la seguridad de los sistemas informáticos, y se configura como un delito de peligro abstracto para la seguridad de estos, que podría, hipotéticamente, suponer un riesgo para la intimidad. Destaca la aportación de TomásValiente Lanuza[26], quien hace hincapié en el hecho de que considerar que el único bien jurídico protegido por esta figura es la intimidad dejaría fuera del ámbito típico el acceso a sistemas informáticos en los que no estuviera alojado ningún dato íntimo. A pesar de esta visión mayoritaria, hay autores[27] que priorizan la ubicación del tipo, lo asimilan al allanamiento de morada y entienden que la conducta típica «acceder y mantenerse» es equivalente a la de dicho delito en el ámbito físico; por tanto, se tutela aquella parcela de la privacidad ligada al domicilio informático.

En conexión directa con esta cuestión está la conducta típica, y aquí es necesario tener en cuenta la modificación del tipo que se realiza en la reforma de 2015[28]. Así, cuando la reforma de 2010[29] introdujo el *intrusismo in-*

---

[24] COLAS TURÉGANO, A. «El delito de intrusismo informático tras la reforma del Código Penal español del 2015». *Revista Boliviana de Derecho,* n.º *21,* enero 2016, pp. 210-229.

[25] *Vid*., entre otros, CARRASCO ANDRINO, M. «El delito de acceso ilícito a los sistemas informáticos». ÁLVAREZ GARCÍA, F. J.; GONZÁLEZ CUSSAC, J. L. (Dirs.). *Comentarios a la reforma penal de 2010.* Valencia: Tirant lo Blanch 2010, pág. 250.

[26] TOMÁS VALIENTE LANUZA, C. *Comentarios al código penal*. GÓMEZ TOMILLO, M. (Dir.). Valladolid: Lex Nova 2011, pp. 802-803.

[27] MORALES GARCÍA, O. *Op. cit*., pág. 185.

[28] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Directiva. 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013.

[29] Ley Orgánica 5/2010**,** de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

formático como conducta delictiva castigaba a quien «por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantuviera dentro del mismo en contra de la voluntad de quien tuviera el legítimo derecho a excluirlo» (antiguo artículo 197.3). Ahora, sin embargo, como exponíamos hace unas líneas, se penaliza al que «sin estar debidamente autorizado, acceda o facilite a otro el acceso[30] al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo» (artículo 197 bis 1).

Resulta destacable, en primer lugar, la modificación relativa a que el acceso no se vincula específicamente a datos o programas concretos, sino al sistema de información (todo o parte)[31]. Con esta modificación, y como señala Colás Turégano, «se acentúa la especial dirección de la figura hacia la tutela de la seguridad alejándose, al propio tiempo, del otro bien jurídico que se pudiera ver afectado con las conductas descritas, la intimidad, al no precisarse que el acceso o mantenimiento lo sea a los datos o programas alojados en un sistema informático», opinión que sustenta en la propia «Exposición de motivos» de la reforma penal de 2015, pues en ella se establece:

> «Se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal y el acceso a otros datos o informaciones que pueden afectar a la privacidad, pero que no están referidos directamente a la intimidad personal: no es lo mismo el acceso al listado personal de contactos, que recabar datos relativos a la versión de software empleado o a la situación de los puertos de entrada a un sistema. Por ello, se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos».

---

[30] «Tendrán cabida dentro de la misma la conducta de todo aquel que haga posible o ayude al acceso de un tercero, produciéndose de esta forma una cierta y criticable ampliación del ámbito de lo punible, pues se eleva a la categoría de autoría lo que hasta el momento solo podía ser calificado como acto de participación, pudiendo abarcar desde supuestos de colaboración necesaria hasta supuestos de mera complicidad, lo que resulta especialmente criticable por la desproporción punitiva a la que conduce, castigando con la misma pena supuestos de diferente lesividad». COLAS TURÉGANO, A. *Op. cit*., pág. 219.

[31] «Todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automatizado de datos informáticos, así como los datos informáticos almacenados, tratados o recuperados o trasmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento». Directiva. 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013.

La cuestión sigue siendo si esa tipificación separada puede desvincularse completamente del derecho a la intimidad (sea de persona física o jurídica)[32]. En nuestra opinión, si bien se tutela el bien jurídico seguridad informática, no puede obviarse sin más la ubicación del tipo, lo que obliga a conectarlo, al menos mínimamente, con la intimidad, lo que lo configuraría, siguiendo a Anarte y Doval[33], como un delito de peligro abstracto para dicho bien jurídico personalísimo, con un adelantamiento, por tanto, de las barreras penales de protección de este.

Esa misma argumentación es recogida por la Audiencia Provincial de Gerona en su Sentencia de 22 de junio de 2015 (358/2015), en la que, en relación con el antiguo artículo 197.3, señala:

> «A diferencia de la mayor parte de los delitos del capítulo, no se trata de una modalidad de descubrimiento, ni tampoco una figura de revelación de secretos, sino más precisamente de intromisión. Ahora bien, incluso a primera vista parece claro que, cuanto más se vincule el artículo 197.3 con el derecho a la intimidad y a los datos personales, más van a superponerse los límites de la intervención penal que proporciona ese precepto con los que ya existían tras la aprobación del Código Penal de 1995 y la reforma del régimen jurídico de los datos personales. De las alternativas que presenta la inserción entre los delitos de descubrimiento de esta nueva infracción, la tesis que registra una mayor adhesión es la de que el artículo 197.3 escapa a la lógica de la tutela directa y única de la intimidad y los datos personales y que marca un nuevo espacio de protección con un objeto jurídico diferenciado: la seguridad o la intangibilidad de los sistemas informáticos. Esta idea se encuentra avalada por la normativa internacional y comparada concordante.
>
> Con respecto a tal objeto, el delito de intrusión se comportaría como una figura de lesión, ya que, en tanto la consumación viene determinada por el acceso o la permanencia, estas conductas suponen evidentemente la vulneración de la seguridad y la intangibilidad de los sistemas informáticos.
>
> En definitiva, con base en razones de orden sistemático, se plantea que el artículo 197.3 sigue estando vinculado con la protección de la intimidad y los datos personales, en tanto que constituirían los bie-

[32] Artículo 200 del CP: «Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código».

[33] ANARTE BORRALLO, E.; DOVAL PAÍS, A. *Derecho penal. Parte especial. Vol. I. La protección penal de los intereses jurídicos personales.* BOIX REIG, J. (Dir.). Madrid: Iustel, pp. 455-456.

> nes jurídicos protegidos. Ahora bien, las conductas que dicha norma sanciona no representan genuinas afecciones de la intimidad y de los datos personales —o sea, descubrimiento o revelación—, sino que se adelanta el umbral típico hasta incorporar estadios previos, lo que convierte al precepto en una figura de peligro en relación con la intimidad y los datos personales, que sería abstracto puesto que se presumiría de la ejecución de las acciones seleccionadas (acceso y mantenimiento)».

Lo que en todo caso no tutela esta figura es el bien jurídico defensa nacional, cuya protección en relación con informaciones secretas o reservadas se articula en el capítulo III del título XXIII («De los delitos de traición y contra la paz o la independencia del Estado y relativos a la defensa nacional»). Para que el mero acceso no consentido a sistemas de defensa pudiese ser incardinado en dicho capítulo (artículos 598 y siguientes) y, por tanto, competencia de la jurisdicción militar a través del artículo 26 del CPM que reenvía a estos, sería necesario que hubiese un presupuesto subjetivo de ánimo de conocer o procurarse los secretos de la defensa nacional, además de que la acción deberá estar dirigida específicamente hacia elementos clasificados como reservados o secretos.

Por tanto, analizando la conducta a la que veníamos refiriéndonos, que es el «mero acceso no autorizado a los sistemas de información de las Fuerzas Armadas», sin ulterior acción de apoderamiento, daño, modificación o revelación de la información que se encuentra en ellos, y sin exigencia de un dolo específico, debemos tener en cuenta todo lo anteriormente expuesto para intentar una tipificación correcta de la conducta.

Así, en este caso nos encontramos con un objeto material específico, que son los sistemas de información de las Fuerzas Armadas. Si optamos por tipificar la conducta como un delito del artículo 197 bis 1, estaríamos ante un delito común, cuyo sujeto activo puede ser tanto paisano como militar. Sin embargo, como venimos señalando, el bien jurídico protegido por este tipo penal nada tiene que ver con la seguridad y defensa nacional, sino que se refiere a la seguridad informática en conexión con la intimidad, ya sea de persona física o jurídica, es decir, como mínimo, a una puesta en peligro abstracto de dicha intimidad. ¿Qué intimidad se ve afectada por el acceso no consentido a sistemas de las Fuerzas Armadas? Si bien sería necesario abordar cada caso concreto, analizando cuáles son los sistemas/datos a los que se accede, parece dudoso que tanto el dolo del autor como la puesta en peligro de los bienes jurídicos vengan referidos a la intimidad del centinela (cuyos datos no tienen por qué estar de ningún modo en los sistemas que monitoriza) o de otros individuos de las FAS. La conducta

afecta a la institución, pero no como persona jurídica cuya intimidad se pone en peligro, sino debido precisamente a su función constitucional (artículo 8 CE), de lo que parece dimanar que la conducta descrita sí podría ser considerada una puesta en peligro del bien jurídico seguridad y defensa nacional.

Siendo así, es decir, eliminando la afectación a la intimidad, y siendo atípico como hemos dicho en el Código Penal común el mero acceso no consentido (sin ulteriores resultados o dolos específicos, más allá del de vulnerar la seguridad del sistema), en relación con los sistemas de defensa nacional, podríamos considerar si la conducta es subsumible en el artículo 34 del CPM, toda vez que el acceso o mantenimiento en el sistema contra la voluntad del que tiene legítimo derecho a excluirlo, esto es, el centinela informático, podría interpretarse como una desobediencia a sus órdenes, y toda vez que como venimos repitiendo ese acceso no pone en potencial peligro un bien jurídico del centinela como persona física o de la empresa pública como persona jurídica, sino la seguridad y defensa nacional. Ahora bien, debemos tener en cuenta que la conducta típica del artículo 197 bis 1 exige la vulneración de medidas de seguridad *ad hoc*.

Ello implica que la conducta debe realizarse vulnerando las medidas de seguridad que estén establecidas *precisamente* para impedir esos comportamientos; es decir, en principio, no únicamente el acceso, sino también la permanencia típica, lo que supone que, de las múltiples medidas de seguridad informática, son relevantes para el tipo solo las que se interponen para evitar la realización de las conductas (como sería el caso de los llamados cortafuegos)[34]. La cuestión es que, si la conducta ya exige la vulneración de medidas de seguridad, será necesario que el autor lleve a cabo una ulterior y más específica vulneración de las instrucciones concretas dadas por el centinela, con las características típicas de una orden, para poder plantear una posible vulneración del artículo 34 del CPM.

Si consideramos que no es posible incardinar la conducta descrita en el artículo 197 bis 1 en el artículo 34 del CPM por exigencias del principio de legalidad, debemos tener en cuenta que el artículo 201 del CP común exige la denuncia de la persona agraviada o de su representante legal, por lo que, salvo que se intentase la excepción contenida en el apartado 201.2 CP: «No será precisa la denuncia exigida […] cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas». Entendiendo

[34] En todo caso, y como señala Morales García, el «nivel de seguridad obviamente no puede ser objeto de descripción típica y deberá vincularse al estado de la técnica en cada comento y a los usos y costumbres de la comunidad». *Op. cit*., pág. 187.

efectivamente que se han visto afectados los intereses generales, no será posible proceder contra un sujeto que haya realizado un mero acceso no consentido a sistemas de las FAS.

Por último, cabe señalar que la conducta a la que venimos haciendo referencia no nos parece subsumible en el artículo 29 del CPM[35]. Entendemos que este artículo exige que el objeto material sea una dependencia física[36], y que el penetrar y permanecer en los sistemas informáticos sería una interpretación que no satisfaría las exigencias de los principios de legalidad y tipicidad.

Procede finalmente hacer una breve referencia al artículo 197 ter del CP ordinario que tipifica la siguiente conducta:

> «Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:
>
> a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o
>
> b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información».

Resulta relevante porque implica la tipificación autónoma de una conducta que anteriormente podría ser abordada como cooperación necesaria o complicidad en la comisión del delito del artículo 197 bis, pero que ahora permite una imputación separada de aquel sujeto (militar o paisano) que facilite un programa, contraseña, etc., concebido para cometer dicho delito. El tipo penal establece un *modus operandi* abierto al recoger cualquier tipo de conducta o modo por el que se faciliten a terceros los medios para la comisión delictiva de los artículos anteriores, sin que las acciones (producción, importación, etc.) presenten diferencias por el hecho de hablar del

---

[35] Artículo 29 del CPM: «El que penetrare o permaneciere en un centro, dependencia o establecimiento militar contra la voluntad expresa o tácita de su jefe, o vulnerare las medidas de seguridad establecidas para la protección de aquellos, será castigado con la pena de tres meses y un día a cuatro años de prisión».

[36] Sentencias de la Sala Quinta n.º 8630/1993 de 13 de diciembre y n.º 2597/1995 de 8 de mayo.

ámbito informático, en relación con el significado común de estos relativo a la producción y tráfico mercantil.

Las conductas vienen referidas a medios concretos idóneos para la comisión de los delitos precedentes, que son programas informáticos, concebidos o adaptados principalmente a tal fin (programas de lanzamiento de *spam,* creación de ordenadores zombis, etc.) y contraseñas de ordenador, códigos de acceso o datos similares para acceder a un sistema de información, enumeración que permite incluir cualquier tipo de elemento informático (dato) que permita dicho acceso.

2.2. El centinela informático como sujeto activo de delitos

2.2.1. La comisión de delitos específicos

De forma paralela o correlativa al amparo proporcionado a la figura del centinela en el CPM debido a su relevante función en la protección de la seguridad y defensa nacional, se penaliza en dicho código la vulneración o quebrantamiento por parte de este de sus obligaciones. Así, el artículo 68, ubicado en la sección 2.ª del capítulo V del título IV recoge los delitos contra los deberes del centinela[37] y establece:

> «1. El centinela que abandonare su puesto será castigado:
>
> 1.º Con la pena de diez a veinticinco años de prisión, cuando tuviere lugar frente al enemigo, rebeldes o sediciosos.
>
> 2.º Con la pena de diez a veinte años de prisión, cuando tuviere lugar en situación de conflicto armado o estado de sitio, fuera de las situaciones expresadas en el apartado anterior, o en circunstancias críticas.
>
> 3.º En los demás casos, con la pena de seis meses a seis años de prisión.
>
> 2. El centinela que incumpliere sus obligaciones, ocasionando grave daño al servicio, será castigado con las penas señaladas en el apartado anterior en su mitad inferior».

[37] También en este caso, el Código de Justicia Militar de 1945 recogía en su artículo 358 el abandono de puesto por cualquier «militar mandando guardia, patrulla, ronda, posición militar o cualquier fuerza en servicio de armas o de transmisiones».

Nuevamente vamos a centrarnos en la figura del centinela informático y las posibles modalidades de comisión por parte de dicha figura de los delitos específicamente vinculados a su función. Así, y entrenado en el análisis del apartado 1 del artículo 68, en relación con el abandono de puesto, no existe, en principio, diferencia alguna con un centinela de puerta en lo que al abandono físico de su servicio se refiere. Esto es, si en el desempeño concreto de sus funciones como operador de las redes informáticas de defensa, el militar físicamente abandonase su puesto frente al terminal informático, colocándose en situación de no poder cumplir con las funciones encomendadas, su conducta sería subsumible en dicho apartado.

Parece, en todo caso, que ese abandono físico tendría que ser relevante en relación con la específica función de operador de redes informáticas, toda vez que, si para el correcto desempeño del servicio, la presencia física en un determinado terminal no es relevante, como lo es en el caso de los centinelas físicos, la conducta podría resultar atípica.

Al respecto del concepto de *abandono* en esta conducta delictiva, la Sala Quinta del TS ha sido consistente en la interpretación ya asentada en la Sentencia de 24 de septiembre de 1993 en la que señalaba que ha de interpretarse:

> «En su significado gramatical de dejación, apartamiento o ausencia de un lugar determinado, o lo que es lo mismo, el desplazamiento material o físico de una persona desde el sitio que ocupaba previamente a otro distinto que le impide realizar el cometido que le correspondía en el lugar primitivo […]. El centinela que deja su puesto y se va a otro lugar distinto desde el que no puede atender el primero, cometerá el delito del vigente artículo 146 del Código Penal Militar, pero no el que permanezca en su puesto o en lugar desde el que pueda vigilarlo, aunque por otras razones incumpla los deberes propios del centinela, pues en este último caso su conducta indiciaria en el supuesto contemplado en el artículo 147, o en las modalidades de infracción disciplinaria para conducta de menor gravedad. Es, por lo tanto, el apartamiento físico del lugar y no la abstracción, pérdida de conciencia o alejamiento psíquico permaneciendo materialmente en el puesto lo que se contempla en el artículo 146».

Por tanto, y como señalábamos, el desplazamiento físico tiene que impedir realizar el cometido que le correspondía como centinela. Si el desempeño de dicho cometido no está ligado a un lugar físico concreto en el caso de un centinela informático, este no cometerá necesariamente el delito del

artículo 68.1 (antiguo 146). Por el contrario, si la ubicación física resulta determinante para su servicio, su alejamiento o desplazamiento podrían ser constitutivos de esta figura delictiva.

En todo caso, no se trata de que el abandono no provoque un daño o perjuicio concreto, puesto que el apartado 1 no exige un resultado, y se consuma con el tipo con el mero alejamiento o desplazamiento físico del centinela, pero sí que esa permanencia física en un puesto esté ligada a su servicio de centinela, lo que es consustancial al centinela físico, pero no necesariamente al informático.

En cuanto al apartado segundo del artículo 68, sí que precisa de un resultado, el grave daño al servicio. En caso contrario, el incumplimiento de los deberes propios del puesto será constitutivos de falta disciplinaria[38]. Será necesario analizar en cada caso concreto las acciones u omisiones llevadas a cabo por el centinela informático a la hora de determinar, en primer lugar, si, en relación con su función específica, suponen un incumplimiento de obligaciones y, en segundo, si el grave perjuicio al servicio se ha producido.

La sentencia de la Sala Quinta del TS de 12 de febrero de 2009 (1065/2009), que recoge la jurisprudencia de la propia sala al respecto del significado de la ocasión del perjuicio, señalaba:

> «Efectivamente, en nuestra sentencia de 21 de marzo de 2004, que cita la sentencia de instancia, decíamos que la exigencia de grave daño del artículo 147 del Código Penal Militar se refiere a la realización del servicio, que puede originar un "incumplimiento total o parcial" y que "ha de ser una alteración que ocasione detrimento, perjuicio, menoscabo (que es en lo que consiste la palabra *daño*), pero que, no requiere que esos daños sean materiales pues, sin ellos, puede el servicio quedar incumplido y, por ende, gravemente dañado" y aunque el delito del artículo 147 del Código Penal Militar exige, ciertamente, la producción de un resultado, "ello no quiere decir que este sea material, pues el *grave daño* lo es con relación al servicio y es obvio que puede originarse un grave daño al servicio sin que se haya producido daño alguno material o que este sea de poca monta". Posteriormente, en sentencia de 14 de febrero de 2006, hemos precisado que el tipo objetivo

[38] Artículo 7.15: «Incumplir las obligaciones del centinela o de otro servicio de armas, transmisiones o guardia de seguridad siempre que no se cause grave daño al servicio, así como abandonar otro tipo de servicios o guardias distintos a los anteriores o colocarse en estado de no poder cumplirlos». Ley Orgánica 8/2014, de 4 de diciembre, de Régimen Disciplinario de las Fuerzas Armadas.

> de este específico delito también se colma, tanto en lo que concierne al incumplimiento de las obligaciones propias del centinela como al resultado jurídico del grave daño para el servicio, en la afectación al mismo servicio que se desempeña, y no en función del riesgo para la seguridad de lo que sea objeto de vigilancia, "porque el daño no es material, sino jurídico, y se refiere al normal desenvolvimiento de la misión del centinela, el cual se impone como consecuencia de la acción contraria a los deberes del servicio"».

De gran relevancia resulta esta cuestión en relación con el incumplimiento del centinela informático de sus deberes, toda vez que cualquier ataque sufrido por las redes de las FAS debido a ese incumplimiento de obligaciones no tiene necesariamente que tener una repercusión material, pero sí causar daño al servicio encomendado. En relación con la existencia de daños, se plantea una cuestión interesante, cual sería la comisión por omisión de los delitos de daños informáticos de los artículos 264 y 264 bis del CP ordinario en la posición de garante del centinela. Así, por ejemplo, si conociendo de la existencia de una bomba lógica el centinela no impide (o no hace todo lo necesario según sus capacidades para impedirlo) su activación, y se produce un resultado grave, podríamos encontrarnos también ante esta modalidad delictiva. Cabe señalar que para que dichas conductas sean relevantes a efectos del CPM tienen que producirse en el contexto del artículo 27 de dicho código y, por tanto, con el ánimo de atentar contra los medios y recursos de la defensa nacional. Siendo esto así, consideramos que es precisamente el tipo de artículo 68 del CPM el que permite una incardinación más adecuada de una conducta omisiva por parte de un centinela informático que, en incumplimiento de sus obligaciones, causa un perjuicio grave al servicio concretado en los resultados de los tipos 264 y 264 bis.

2.2.2. Comisión delictiva por extralimitaciones en su actuación

Al margen de cometer un abandono de puesto o un incumplimiento de obligaciones en el desempeño de su función de centinela, no queremos dejar de analizar la posible comisión por parte del centinela informático de otros tipos penales debido a un exceso o extralimitación en el ejercicio de sus cometidos.

Nuevamente cabe partir del abordaje del asunto desde la figura del centinela de puertas, y en este sentido debemos volver a mencionar la normati-

va complementaria, a la que ya nos habíamos referido a la hora de abordar el concepto de centinela.

Así, el artículo 25.3 del Real Decreto 194/2010, de 26 de febrero, por el que se aprueban las Normas sobre Seguridad en las Fuerzas Armadas establece: «Cuando resulte amenazada la seguridad de su puesto, su persona o el cumplimiento de la consigna, previa las conminaciones dirigidas al potencial agresor para que abandone su actitud y de la advertencia de que se halla ante un centinela, podrá hacer uso gradual y proporcionado de su arma, procurando causar el menor daño posible». Cuestión que es reproducida por el apartado 2 del artículo 88 del Régimen Interior del Ejército de Tierra, que señala: «En el caso del centinela, si resulta amenazada la seguridad del puesto que guarda, su persona o el cumplimiento de la consigna asignada, podrá hacer uso gradual y proporcionado de su arma, procurando causar el menor daño posible».

Es decir, para garantizar la eficacia de su función se establece la posibilidad del uso del arma de forma gradual y proporcionada. Se establece que ese uso puede realizarse en caso de que resulte amenazada no solo la seguridad del puesto o el cumplimiento de la consigna asignada ―en seguimiento de la definición legal del artículo 4 del CPM―, sino también la persona del centinela[39].

En el caso de un centinela informático, y salvo que se produzca un asalto de carácter físico, no es la persona, sino la seguridad y el cumplimiento de la consigna recibida o las funciones inherentes al puesto lo que podría verse amenazado. ¿Cuáles son, por tanto, los márgenes y limitaciones de actuación de este? El centinela informático no tiene un arma física (o al menos ello no es relevante para su función informática), pero sí es posible que tenga unas cibercapacidades a su disposición que puedan ser consideradas como tales, tal y como se ha establecido en la interpretación hecha en el ámbito del derecho internacional de los Convenios de Ginebra y el uso de armas cibernéticas (*malware,* bombas lógicas*, botnets*, etc.)[40].

---

[39] En todo caso, el centinela, al margen de esta regulación reglamentaria, tiene además un derecho a la legítima defensa que, como sabemos, en nuestro ordenamiento jurídico opera como eximente que deberá cumplir determinados requisitos, tal y como se establece en el artículo 20. 4.º del CP.

[40] En la *Nuclear Weapons Advisory Opinion* de la Corte Internacional de Justicia se establece que «los principios y reglas del derecho humanitario se aplican a todas las formas de guerra y a todos los tipos de armas, del pasado, del presente y del futuro», postura que se ha adoptado en el ámbito de la ciberdefensa. Así, hablaríamos de cualquier ciberdispositivo, material, instrumento, mecanismo, equipo o *software* usado o diseñado para poder llevar a cabo algún tipo de ataque informático. *Vid*. SCHMITT, M. N. (ed.). *Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press 2013.

Consideramos que, amparado por su obligación de guardar la seguridad del puesto que se le ha confiado (las redes/sistemas concretos), el centinela informático podrá llevar a cabo aquellas acciones necesarias para impedir la vulneración de esa seguridad *causando el menor daño posible*. Pero, al igual que no resulta penalmente admisible que, una vez pasada una amenaza un centinela de puertas busque, investigue y llegue a atacar al que intentó o consiguió entrar en la instalación (y desapareciera posteriormente), no puede un operador de redes emplear los conocimientos y herramientas (armas) puestos a su disposición por las Fuerzas Armadas para llevar a cabo actuaciones que podrían suponer la comisión de delitos comunes, como el del artículo 197 bis 1 que hemos analizado anteriormente[41] o de daños informáticos de los artículo 264 y 264 bis.

Es decir, en la detección de incidentes, intrusiones, problemas de seguridad informática, etc., los operadores de redes informáticas deben usar sus cibercapacidades para cumplir con sus obligaciones de mantener la seguridad, pero no para llevar a cabo investigaciones, interceptaciones de datos, registros remotos, etc., que son competencia de las fuerzas y cuerpos de seguridad del Estado bajo la dirección judicial, ni tampoco usar *malware* u otras herramientas informáticas contra sistemas ajenos en acciones de ataque o represalia produciendo daños informáticos o intromisiones en la intimidad y, por tanto, pudiendo ser sujetos activos de los delitos señalados del CP común.

En este sentido, cabe aquí hacer referencia a la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el Fortalecimiento de las Garantías Procesales y la Regulación de las Medidas de Investigación Tecnológica**,** toda vez que con anterioridad a esta no se regulaban técnicas específicas para la investigación tecnológica en nuestra legislación procesal (ni ordinaria ni militar) , sino que era lo habitual la aplicación de otras disposiciones que regulaban aspectos como la intervención de la correspondencia o de las comunicaciones telefónicas. Ahora, sin embargo, dentro del título VIII, relativo a las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución, se recogen dichas medidas concretas, que serán de aplicación al ámbito del proceso penal militar, en virtud del carácter supletorio de la Ley de Enjuiciamiento Criminal (LECrim) en todo aquello no regula-

[41] Puede llegar a ser aplicable la agravación específica del artículo 198: «La autoridad o funcionario público que, fuera de los casos permitidos por la ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años».

do específicamente en la Ley Procesal Militar 2/1989, de 13 de abril, como es el caso[42].

Como la propia denominación del título VIII indica, todas las medidas, tecnológicas o no, que se regulan en los artículos 545 a 588 octies son susceptibles de incidir en el derecho a la intimidad, la inviolabilidad del domicilio y el secreto de las comunicaciones. Es lo que lleva a que el inicio del capítulo IV de la LECrim, específicamente dedicado a medidas tecnológicas, se centre en una serie de disposiciones comunes que hacen hincapié en los principios rectores de especialidad, idoneidad, necesidad y excepcionalidad, y proporcionalidad de estas (artículo 588 bis a), pero, además, a que se establezcan requisitos muy concretos de la petición por parte de Policía Judicial o Ministerio Fiscal, así como de la propia resolución judicial, su duración y control, que en nuestra opinión responden a la necesaria toma en consideración de que las capacidades tecnológicas, por muy avanzadas y útiles que pudieran resultar, no se usen de forma expansiva en detrimento de los derechos de los ciudadanos.

Por tanto, para que la realización de estas investigaciones y la aportación de los resultados de estas puedan configurarse como una prueba válida a un proceso penal con todas las garantías, deben ser llevadas a cabo por los sujetos competentes para ello y bajo la dirección judicial. Tanto los centinelas informáticos como otros sujetos militares en otras funciones informáticas tienen encomendada la tarea de garantizar la seguridad de sistemas, datos e informaciones. Sus capacidades y conocimientos deben estar dirigidos a esa función primordial de seguridad y defensa, para lo cual se podrán aplicar las técnicas precisas para diagnosticar los incidentes y aplicar las soluciones de seguridad informática precisas. Ahora bien, entre esas técnicas nunca podrá estar la realización de acciones que son competencia exclusiva de las fuerzas y cuerpos de seguridad del Estado, bajo dirección de la autoridad judicial, como hemos señalado.

De tal forma que, por poner un ejemplo, ante un incidente de seguridad, las capacidades del MCCD no pueden emplearse para llevar a cabo un registro remoto, ya que eso podría suponer, como hemos señalado, la comisión de delitos como los tipificados en los artículos 197 y siguientes del CP ordinario o de daños informáticos (artículos 264266 CP), entre otros, salvo que nos encontremos ante una situación de ataque armado por parte de otro Estado o sus agentes y ello, en aplicación del derecho internacional, legitimase una respuesta agresiva, que en todo caso, y de conformidad con

[42] La Ley Procesal Militar regula única y brevemente la entrada y registro en lugar cerrado y la intervención de libros, papeles y comunicaciones en los artículos 185 a 189.

la normativa internacional, sería bajo los requisitos de necesidad y proporcionalidad.

Por otro lado, el desarrollo de capacidades de informática forense puede ser, y de hecho es, extremadamente útil para la mejora de la defensa de los sistemas, pero su utilidad en un proceso penal está directamente vinculada a la licitud y fiabilidad de los peritajes realizados, de forma que las actuaciones autónomas, sin intervención de las fuerzas y cuerpos de seguridad del Estado y la autoridad judicial correspondiente, servirán de poco para el enjuiciamiento de los hechos.

Por último, no queremos dejar de apuntar que la extralimitación de los centinelas informáticos en sus facultades a la hora de desempeñar su labor, y al hilo de lo apuntado sobre las situaciones de conflicto armado, también podría llevar a la comisión de otros ilícitos penales, como los delitos contra las personas y bienes protegidos en dicho contexto. Por ejemplo, el artículo 610 del CP[43] tipifica la prohibición del derecho internacional del empleo de medios y métodos de guerra prohibidos[44]:

> «El que, con ocasión de un conflicto armado, emplee u ordene emplear métodos o medios de combate prohibidos o destinados a causar sufrimientos innecesarios o males superfluos, así como aquellos concebidos para causar o de los que fundamentalmente quepa prever que causen daños extensos, duraderos y graves al medio ambiente natural, comprometiendo la salud o la supervivencia de la población, u ordene no dar cuartel, será castigado con la pena de prisión de 10 a 15 años, sin perjuicio de la pena que corresponda por los resultados producidos».

En el ámbito cibernético, en el caso de un *botnet* empleado para llevar a cabo un ataque de denegación de servicio (DoS), el *botnet* sería el

---

[43] El artículo 9 del CPM establece como delitos militares los tipificados en el CP ordinario como «delitos contra las personas y bienes protegidos en caso de conflicto armado», incluidas las disposiciones comunes, si bien deberán cometerse «con abuso de facultades o infracción de los deberes establecidos en la Ley Orgánica 9/2011, de 27 de julio, de Derechos y Deberes de los Miembros de las Fuerzas Armadas o en la Ley Orgánica 11/2007, de 22 de octubre, reguladora de los Derechos y Deberes de los Miembros de la Guardia Civil».

[44] *Vid*. artículo 23 de la Convención de la Haya de 1907 y los artículos 35 y 36 del Protocolo I de 1977 a los Convenios de Ginebra de 1949; existen, además, múltiples convenciones relativas a la cuestión, como la Convención sobre la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de Armas Químicas y sobre su Destrucción; la Convención sobre la Prohibición del Desarrollo, la Producción y el Almacenamiento de Armas Bacteriológicas (Biológicas) y Toxínicas y sobre su Destrucción; la Convención sobre la Prohibición de Empleo, Almacenamiento, Producción y Trasferencia de Minas Antipersonales y sobre su Destrucción; la Convención sobre Municiones de Racimo, etc.

medio de combate y el DoS el método. Si bien debemos significar como punto de partida que las armas cibernéticas no están, en su conjunto y *a priori*, prohibidas, como puede ser el caso de las municiones de racimo o las armas químicas, y, por tanto, será necesario analizar el diseño concreto de un determinado *malware* o su capacidad concreta en un determinado contexto para determinar la comisión delictiva. Pero la cuestión es que un empleo inadecuado de las capacidades tecnológicas por parte de los centinelas informáticos en un contexto de conflicto armado podría acarrear responsabilidades penales tanto nacionales como internacionales, al igual que cualquier otra extralimitación o abuso de capacidades en ese mismo contexto.

3. CONCLUSIÓN

El avance tecnológico incide en todos los ámbitos de la realidad convirtiéndose en un aspecto de extrema relevancia a la hora de configurar la protección penal de bienes jurídicos, incluidos aquellos de especial relevancia en el ámbito militar, como la seguridad y defensa nacional. Ello ha hecho necesaria la adaptación de las normativas penales y procesales de los Estados a lo largo de los últimos años, incluida la normativa penal militar.

En este sentido, dentro de las novedades del Código Penal Militar de 2015 destaca la inclusión en el nuevo texto penal de la figura del centinela informático en una acertada valoración de la relevancia de su función específica; se le proporciona protección penal y se le hace también sujeto sometido a una responsabilidad penal. Ahora bien, del análisis realizado se desprende que precisamente las peculiaridades de sus funciones de salvaguardia podrían exigir de un tratamiento diferenciado de esta figura que permita, en atención al principio de legalidad, desterrar las dudas sobre la comisión de delitos que pueden afectar a dichas funciones y a la seguridad de las instalaciones, pero quedar impunes o bajo la competencia de la jurisdicción ordinaria. Del mismo modo, la exigencia de responsabilidad podría resultar más amplia, específica y diferenciada que en el caso de centinelas de puerta o incluso de operadores de redes de trasmisiones, dado su conocimiento y capacidad para llevar a cabo acciones que, bajo la consigna de la protección de la seguridad y defensa nacional, podrían llegar a constituir conductas delictivas.

Si bien los centinelas de puertas siguen teniendo una función de primera magnitud en las FAS, la relevancia de los operadores de redes para la seguridad de estas y el mantenimiento de sus capacidades para el cum-

plimiento de su función constitucional resultará, dado el avance de la tecnología y su penetración en el ámbito militar, cada vez más importante, lo que hace necesario profundizar en los aspectos señalados en las anteriores líneas, a fin de proporcionar límites adecuados de actuación, pero también capacidades tanto técnicas como legales para luchar contra fenómenos delictivos que pueden poner en peligro la seguridad y defensa nacional, y que en la actualidad no encuentran suficiente cobertura legal.

BIBLIOGRAFÍA

LIBROS, CAPÍTULOS DE LIBROS Y ARTÍCULOS

CARRASCO ANDRINO, M. «El delito de acceso ilícito a los sistemas informáticos». ÁLVAREZ GARCÍA, F. J.; GONZÁLEZ CUSSAC, J. L. (Dirs.). *Comentarios a la reforma penal de 2010.* Valencia: Tirant lo Blanch 2010, pp. 249-256.

— «El acceso ilícito a un sistema informático». ÁLVAREZ GARCÍA, F. J.; MANJÓN CABEZA OLMEDA, A.; VENTURA PÜSCHEL, A. *La adecuación del derecho penal español al ordenamiento de la Unión Europea: la política criminal europea*. Valencia: Tirant Lo Blanch 2009.

CEREZO MIR, J. *Curso de derecho penal español. Parte general*. Tomo II. Madrid: Tecnos 2000.

COLAS TURÉGANO, A. «El delito de intrusismo informático tras la reforma del Código Penal español del 2015». *Revista Boliviana de Derecho,* n.º *21,* enero 2016, pp. 210-229.

CONDE-PUMPIDO TOURÓN, C. (2016). «La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (artículos 588 sexies y 588 septieslecrim)» **[en línea]**. *Jornadas de especialistas en criminalidad informática*. Disponible en www.cej-mjusticia.es.

DE LA CUESTA ARZAMENDI, J. J.; PÉREZ MACHÍO, A. U.; SAN JUAN GUILLÉN, C. «Aproximaciones criminológicas a la realidad de los ciberdelitos». DE LA CUESTA ARZAMENDI, J. J. (Dir.). *Derecho penal informático*. Madrid: Civitas 2010.

DE LA MATA BARRANCO, N. J. *Derecho penal europeo y legislación española: Las reformas del Código Penal*. Valencia: Tirant lo Blanch 2015.

DE TOMÁS MORALES, S.; VELÁZQUEZ Y ORTIZ, A. «La responsabilidad del mando en la conducción de operaciones durante la ciberguerra». Ministerio de Defensa. *Revista Española de Derecho Militar*, n.º 100, enero-diciembre 2013, Madrid, pp. 117150.

DÍAZ GÓMEZ, A. «El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest**».** Universidad de la Rioja. *REDUR,* 8, diciembre 2010, pp. 169-203.

GÓMEZ TOMILLO, M, *Responsabilidad penal y civil de los delitos cometidos a través de Internet*. Cizur: Aranzadi 2004.

GONZÁLEZ RUS, J. J. «III. Delitos contra la Seguridad exterior e interior del Estado; de las falsedades». COBO DEL ROSAL, M. (Dir.). *Manual de Derecho Penal (Parte Especial)*. Madrid: AANV 1994.

GONZÁLEZ-CUELLAR SERRANO, N.; MARCHENA GÓMEZ, M. *La reforma de la ley de enjuiciamiento criminal de 2015*. Madrid: Castillo de Luna 2015.

HERNÁNDEZ DÍAZ, L. «El delito informático». Universidad del País Vasco. *EGUZKILORE*, n.º 23, diciembre 2009, pp. 169-203.

JEWKES, Y.; JAR, M. (eds.). *Handbook of Internet Crime*. Devon: William publishing 2010.

MARCHENA GÓMEZ, M. (2001), «El sabotaje informático: entre los delitos de daños y desórdenes públicos». LÓPEZ ORTEGA, J. J. (Dir.). *Cuadernos de Derecho Judicial*, n.º 10, CGPJ, Madrid, pp. 353-366.

MIRÓ LLINARES, F. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons 2012.

MORALES GARCÍA, O. «Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (artículo 197 3 y 8 264 y 258)».

QUINTERO OLIVARES, G. *La reforma penal de 2010: Análisis y comentarios*. Madrid: Aranzadi 2010, pp.181-194.

PASTRANA I ICART, L. I. «Los secretos en los delitos relativos a la defensa nacional (comentario a los artículos 598 a 603 CP)». *Anuario de Derecho Penal y Ciencias Penales,* vol. LL, 1998, pp. 273-317.

QUERALT JIMÉNEZ, J. J. *Derecho penal español. Parte especial.* 6.ª edición. Barcelona: Atelier 2010.

RODRÍGUEZ DEVESA, M.; A. SERRANO GÓMEZ, A. *Derecho penal español. Parte especial*. Madrid: Dykinson 1992.

RODRÍGUEZ MOURULLO, G.; GALLO ALONSO, J.; LASCURAÍN SÁNCHEZ, J. A. «Derecho penal e internet». FERNÁNDEZ ORDÓÑEZ, M.; CREMADES GARCÍA, J.; ILLESCAS ORTIZ, R. *Régimen jurídico de internet*. Wolters Kluwer 2001, pp. 255-307.

RODRÍGUEZ LAÍNZ, J. L. «Tres cuestiones polémicas sobre el registro de dispositivos electrónicos de almacenamiento masivos de información» [en línea]. *Sepin*, septiembre 2016. Disponible en www.sepin.es.

ROMEO CASABONA, C. M. *Poder informático y seguridad jurídica*, *la función tutelar del derecho penal ante las nuevas tecnologías de la información*. Madrid: Fundesco 1988.

— (coord.) *El cibercrimen: nuevos retos jurídicopenales, nuevas respuestas políticocriminales*. Madrid: Comares 2006.

ROVIRA DEL CANTO, E. «Las nuevas pruebas telemáticas y digitales. Especialidades de la prueba en delitos cometidos por internet». Centro de Estudios Jurídicos de la Administración de Justicia. *Estudios Jurídicos*. *Ministerio Fiscal*, n.º 1, 2003, pp. 277-326.

SALVADORI, I. *Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado*. ADPCP, vol. LXIV, 2011.

SCHMITT, M. N. (ed.). *Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press 2013.

TOMÁS VALIENTE LANUZA, C. *Comentarios al código penal*. GÓMEZ TOMILLO, M. (Dir.). Valladolid: Lex Nova 2011.

REFERENCIAS NORMATIVAS

Circular 1/2013 de la Fiscalía General del Estado de 11 de enero sobre pautas en relación con la intervención de las comunicaciones telefónicas.

Código de Justicia Militar de 1945.

Convenio sobre Ciberdelincuencia de 23 de noviembre de 2001 del Consejo de Europa.

Instrucción 2/2011 de la Fiscalía General del Estado, Sobre el fiscal de sala de criminalidad informática de las fiscalías, de 11 de octubre de 2011.

Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
Real Decreto 194/2010, de 26 de febrero, por el que se aprueban las Normas sobre Seguridad en las Fuerzas Armadas.

JURISPRUDENCIA

STS de la Sala Quinta n.º 8630/1993 de 13 de diciembre.
STS de la Sala Quinta n.º 2597/1995 de 8 de mayo.
STS de la Sala Quinta n.º 7825/2002 de 25 de noviembre.
STS de la Sala Quinta n.º 7311/2007, del 5 de noviembre.
STS de la Sala Quinta n.º 1065/2009, de 12 de febrero.
STS de la Sala Quinta n.º 496/2013, de 23 de enero.
STS de la Sala Quinta n.º 1824/2013 de 16 de abril.
Sentencia de la Audiencia Provincial de Gerona n.º 358/2015 de 22 de junio.