«EL DELITO INFORMÁTICO Y SU INCIDENCIA EN EL CÓDIGO PENAL MILITAR»

Marcelo Ortega Gutiérrez-Maturana
Coronel auditor

SUMARIO

1. INTRODUCCIÓN

Para situar adecuadamente el objeto de nuestro estudio —ilícitos militares cometidos a través de internet o con ocasión del uso de las nuevas tecnologías— habremos de hacer referencia, en primer lugar al marco en que nos movemos, así examinaremos brevemente: el denominado Derecho Informático, describiremos, siquiera, someramente, la evolución de las conductas delictivas vinculadas a las nuevas tecnologías, para llegar al estado actual de la cuestión, ocupándonos de los aspectos principales que presenta. Una vez en este punto, afrontaremos la conceptualización del Delito Informático y su clasificación, desde un punto de vista, eminentemente, práctico y apegado al objeto de nuestro estudio. Más adelante, nos ocuparemos de un aspecto capital en la materia cual es la necesaria especialización, de los llamados a perseguir estos delitos, en nuestro caso Policía Judicial, Ministerio Fiscal y Jueces, para tras detallar la principal normativa en la materia, entrar, de lleno, en los ilícitos propiamente militares.

1.1 «Derecho informático»

La delincuencia informática forma parte de lo que se ha denominado *«Derecho Informático»*, este es entendido como un conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la sociedad, cuya materia incluiría: 1.º el régimen jurídico del software; 2.º el derecho aplicable a las Redes de transmisión de datos; 3.º los documentos electrónicos; 4.º los contratos electrónicos; 5.º el régimen jurídico de las bases de datos; 6.º el derecho de la denominada «*privacy»;* 7.º los

delitos informáticos; y 8.º con carácter residual, otras conductas nacidas del uso de los ordenadores y de las redes de transmisión de datos[1].

Existían distintas opciones posibles, sin embargo, se ha optado por crear una nueva rama del Derecho dedicada exclusivamente al estudio de estos aspectos, y ello porque la complejidad de las relaciones informáticas, su crecimiento desmesurado o el hecho de que en el estudio de estas nuevas relaciones sea necesaria moverse de una rama del ordenamiento jurídico a otra constantemente (civil, penal, procesal, administrativa o laboral). Esta nueva rama del ordenamiento jurídico regularía las relaciones, cualesquiera, vinculadas con la informática y tendría como característica, precisamente, el hecho de que en la disciplina confluyan normas administrativas, civiles, procesales, penales, laborales, etc.

1.2. Las TIC (tecnologías de la información y comunicación), hitos en su evolución y aparición de nuevas conductas y formas de comisión ilícitas o delictivas

Ciñéndonos al marco del Derecho Penal y Procesal, el primer problema con el que nos encontramos a la hora de afrontar el análisis de los delitos informáticos es intentar describir su contenido. No resulta fácil determinar qué debe entenderse por delito informático y qué conductas pueden considerarse incluidas en el mismo; de hecho, ni siquiera la doctrina encuentra un concepto unitario de delito informático y las discrepancias en torno al mismo han llegado incluso a propiciar que algunos autores admitan la imposibilidad de dar una definición del mismo y renuncien a ello[2]. La doctrina ha debatido durante años si nos encontramos ante una categoría que pueda denominarse *«delito informático»* o si, por el contrario, se deben utilizar expresiones que carezcan de un matiz jurídico-positivo, haciendo alusión, más bien, a categorías criminológicas: así las expresiones delincuencia informática, criminalidad informática o delitos informáticos.

En gran parte el problema viene propiciado por la vertiginosa velocidad con la que evolucionan las nuevas tecnologías y el consiguiente cam-

[1] Seguiremos en este apartado el desarrollo que propone HERNÁNDEZ DÍAZ, L., «*El delito informático»*, Revista Eguzkilore 23, 2009, pp. 227- 243.

[2] En tal sentido, FERREYROS SOTO, C., *«Aspectos metodológicos del delito informático»*, en Informática y derecho: Revista iberoamericana de derecho informático, 9-11, 1996 pp. 407 ss., que, prescinde de una conceptuación, limitándose a enumerar las peculiaridades que presenta el conjunto de comportamientos a que puede venir referida la expresión.

bio y desarrollo constante, igualmente rápido, de las conductas delictivas vinculadas a estas.

Antes de intentar exponer un concepto de delito o delitos informático parece oportuno, que hagamos un repaso, si bien muy general, de las principales etapas por las que ha discurrido la implantación de las nuevas tecnologías y del modo en que, en consecuencia, ha ido apareciendo el nuevo elenco de conductas lesivas de derechos vinculadas con la informática y la telemática.

Utilizaremos, para sistematizar la evolución de las conductas delictivas (o merecedoras de serlo) vinculadas con las TIC, el estudio, sobre la misma, contenido en el *«Informe sobre la situación del crimen organizado en Europa»* realizado por el Consejo de Europa en 2004[3], distinguiendo las siguientes etapas:

1.2.1. Años sesenta

En esa época, inicios de la informática, se produce una ingente acumulación de datos de carácter personal de la ciudadanía por parte de los gobiernos, aun cuando no estaba masificado el uso de los ordenadores, hace que comiencen las preocupaciones en torno al carácter reservado, la acumulación y el uso que podría hacerse de estos datos. Nace así el concepto de «*privacy»* y del derecho a la misma, que va más allá del tradicional de intimidad y que regula la *acumulación en las bases de datos, de carácter informático o no, de información sobre los individuos y el uso que se hace de ella,* así como la capacidad de decisión de cada ciudadano respecto a qué datos referentes a su persona deben ser compartidos o públicos. Ya en los años sesenta comienzan las primeras discusiones en torno a esta cuestión, sobre todo en materia civil y administrativa, planteándose el debate, en los años siguientes, también en términos penales.

1.2.2. Década de los setenta

Durante ese periodo, la difusión de los ordenadores en el mundo empresarial supuso que la mayoría de las manifestaciones de la delincuencia

[3] Consejo de Europa, *«Organised crime in Europe: the threat of cybercrime. Situation report 2004»*, Francia, 2005, pp. 83 a 94.

informática tuviesen relación con la *delincuencia económica*, siendo las más comunes el fraude informático, la manipulación de datos, sabotajes informáticos, espionajes empresariales, etc. Hasta el punto de que en este periodo eran estas nuevas modalidades de delincuencia económica las que integraban el concepto de delito informático; o, al menos, estas eran las principales manifestaciones del mismo.

1.2.3. En los años ochenta

La generalización de los ordenadores personales entre la población trajo consigo, al mismo tiempo, el surgimiento de la piratería del software de los mismos, dando comienzo así a las primeras *infracciones contra la propiedad intelectual* que se generalizarían a finales de los años noventa, extendiéndose además a productos como música, fotografías o películas.

1.2.4. Los noventa

La expansión de Internet en la década de los noventa llevó aparejado el surgimiento de un nuevo método para *difundir contenidos ilegales o dañosos, tales como pornografía infantil o discursos racistas o xenófobos*. Serán precisamente las conductas vinculadas a la difusión de contenidos ilícitos las que más pueden aprovecharse de la enorme implantación que tiene la Red a nivel mundial, así como de sus características técnicas que dificultan su descubrimiento, persecución y prueba.

En este período también se consolida la *dependencia que los gobiernos y organismos internacionales tienen de los sistemas informáticos, tanto para su buen funcionamiento como para el almacenamiento de datos importantes y/o secretos* y ello pondrá en el punto de mira para la comisión de delitos que atenten contra la seguridad del Estado, como la comisión de ataques terroristas a través de la Red, a los sistemas informáticos de estos Entes.

1.3. Situación actual

La revolución tecnológica en la que nos hallamos inmersos con la aparición de la última generación de telefonía móvil multifuncional y de aparatos

asistentes personales digitales (PDA) asimismo multifuncionales, y en las que, el clásico intercambio de palabras o pensamientos a través del teléfono o el correo ordinario, ha sido superado, no solo por el intercambio de datos, en gran cantidad y con mayor celeridad, comprendiendo voz, texto, música, fotografías o videos, sino también con la capacidad de producción, procesamiento y transmisión de datos, propia de un equipo informático y utilizando medios telemáticos, con conexión remota al sistema informatizado de nuestra vivienda (domótica), y principalmente a Internet, y, no solo entre personas y ordenadores, sino incluso entre ordenadores sin intervención directa del ser humano, en lo que lo importante es no tanto si se ha establecido una conexión directa entre el emisor y el receptor, sino que los datos entren en la red con una dirección de destino o que puedan ser accesibles para cualquiera que quiera conocerlos u obtenerlos. Siguiendo a ROVIRA DEL CANTO, podemos distinguir como aspectos principales de esta evolución[4]:

1.3.1. La facilidad en el acceso, búsqueda, intercambio y difusión de información

En el último decenio ha aumentado claramente, siendo incluso promovido por la administración y organismos públicos, la facilidad en el acceso, búsqueda, intercambio y difusión de información contenida en redes y sistemas informáticos, superando las distancias geográficas, y ha llevado a un *crecimiento explosivo en la cantidad de información accesible*, así como el conocimiento generalizado de que puede ser obtenida de dichos sistemas, siendo significativa la progresiva generalización en el uso del correo electrónico y el acceso y consulta, a través de Internet, de numerosos sitios o páginas web de distintas partes del mundo.

1.3.2. El aumento del riesgo de perpetración de actos ilícitos

La segunda consecuencia es que, esos progresos, han tenido también su reflejo no solo en los ámbitos civil, social y administrativo, sino tam-

[4] 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-2003. C. E. J. A. J. Madrid. 2003.

bién en la delincuencia y criminalidad, propiciando asimismo un aumento del riesgo de perpetración de actos ilícitos. Han aparecido *nuevos tipos de acciones ilícitas, así como nuevas modalidades y peculiaridades en la comisión de delitos tradicionales*, y las conductas criminales pueden ser de mayor entidad y trascendencia puesto que no están restringidas por limitaciones geográficas o fronteras nacionales.

1.3.3. La globalización del fenómeno

La mayor potencia de los sistemas informáticos, sus mayores prestaciones y su generalizada disponibilidad para cualquier persona, unido al crecimiento de las redes y sistemas telemáticos, sobre todo las abiertas, como Internet, la utilización generalizada de terminales móviles de telecomunicación personal, consolidándose asimismo una *«telecomunicación personalizada global de masas»*, y la interconexidad entre sistemas informáticos y de telecomunicación, en lo que se denomina telemática, con desaparición material no ya de las fronteras sino de todo tipo de barreras espacio-temporales, *permitiendo obtener, procesar y transmitir la información en tiempo real en y a cualquier parte del planeta, favoreciendo además la descentralización de la información, la interrelación, incluso simultánea de múltiples sujetos ubicados en distintos lugares lejanos geográficamente entre sí*.

1.3.4. El ciberespacio

Esta coincidencia que apuntamos tiene lugar en un nuevo espacio virtual, el ciberespacio, que llega a producir nuevas formas de realidad y en el que, como afirma MORON LERMA[5], *«lo real puede convertirse en falso, el original, en copia y el ser, en identidad virtual»*, con independencia de un punto concreto del planeta, ha supuesto la producción de cambios tanto respecto al autor como a la víctima de los ataques informáticos y telemáticos, pues *los delitos informáticos hoy en día no solo pueden ser cometidos por cualquiera, sino que también amenazan a cualquier ciudadano*, y ha

[5] MORÓN LERMA, E., «*Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red»*, colección RdPP monografía, Ed. Aranzadi, Pamplona, 1999, p. 79.

desarrollado nuevos supuestos de comisión delictiva, como, por ejemplo los abusos telefónicos, la interceptación de datos o sistemas de comunicación, las acciones ofensivas contra el honor, la emisión de contenidos ilícitos y nocivos, y las manipulaciones en Internet.

1.3.5. Nuevos intereses y bienes jurídicamente protegibles

Actualmente *«lo informático»* se constituye no solo en un medio sino incluso en un objeto potencial para la realización de ilícitos estrictamente telemáticos o cibernéticos. Esa cada vez más frecuente interrelación personal, comercial, e incluso delictiva, de carácter global y transfronterizo, y la existencia de idénticos y *nuevos intereses y bienes jurídicamente protegibles, como la información informatizada, los datos que la representan, los sistemas y redes por donde fluye, se transmite, elabora, procesa, contiene, obtiene y almacena*, para un conjunto cada vez mayor de Estados, constituye el gran reto del cambio social del siglo XXI, y hace necesaria de *armonización internacional de las legislaciones estatales, y no solo la penal sustantiva sino por supuesto también de la procesal en cuanto a la licitud y eficacia de los medios de obtención de pruebas de los delitos cometidos a través de los nuevos sistemas telemáticos y la validez y suficiencia de las pruebas electrónicas y telemáticas*. Y las redes telemáticas e Internet traen consigo un nuevo concepto superador del tradicional delito informático, el de ciberdelito o delito cibernético.

1.3.6. *Libertad sí, pero no impunidad*

Es pertinente traer a colación la máxima, mantenida por ROVIRA DEL CANTO, como respuesta a los posicionamientos doctrinales o sociales contrarios a cualquier tipo de regulación de Internet y que normalmente lleva aparejada un menor desvalor de las acciones ilícitas verificadas en la red y el ciberespacio y por tanto de la Ciberdelincuencia[6]: «*LIBERTAD SÍ, PERO NO IMPUNIDAD»*.

La red Internet no ha sido concebida para el comercio electrónico, los contratos, la venta de contenidos protegidos por los derechos de autor (músi-

[6] ROVIRA DEL CANTO, E., «*Las nuevas pruebas...*», op. cit.,p. 283.

ca, imágenes y películas), las transferencias de capitales y otras operaciones económicas que exigen unas medidas de seguridad específicas. Inicialmente se utilizaba con fines militares y universitarios: la encriptación mediante largas claves, en el primer caso, y la publicación de resultados experimentales y de bases de datos científicos sin codificar, en el segundo, respondían a las necesidades. Más adelante se extendió la utilización *«libertaria»* de Internet, y después con fines comerciales, financieros, tecnológicos, industriales y lúdicos, sin contar los sitios pornográficos, que generan importantes ingresos y, de hecho, junto con los juegos en línea, son fuente de considerables evoluciones tecnológicas, en particular en materia de calidad de imagen y alta velocidad o de sistemas de pago seguros, anónimos o no.

Todos estos modos de utilización siguen coexistiendo y gradualmente surgen otros nuevos. No obstante, partes cada vez mayores de las redes e Internet constituyen los pilares del funcionamiento de la sociedad y de la economía, contribuyen de manera decisiva al desarrollo social y la seguridad nacional y exigen un mayor nivel de seguridad en función de la naturaleza de los datos transmitidos y las operaciones efectuadas, respetando la intimidad de las personas y sin cuestionar el principio básico de Internet, es decir, la libre circulación de información y el intercambio abierto de datos, ideas, resultados científicos, etc. E incluso se ha convertido en un medio a través del cual se realizan acciones de guerra electrónica, o económica, como hemos visto en las informaciones recientes relativas a ataques cibernéticos realizados, presuntamente, por el Ejército de la República Popular China, o, más recientemente, el de la República Popular de Corea, o la intercepción masiva de comunicaciones realizada por la Agencia Nacional de Inteligencia norteamericana[7] o el espionaje generalizado de las delegaciones participantes en la Cumbre del G-20 celebrada en 2009 en el Reino Unido[8].

---

[7] http://observatorio.cisde.es/?p=7476#more-7476 Ello ha llevado a la Unión Europea junio 12, 2013 Redacción**. «**La Comisión Europea ha expresado su preocupación por las recientes informaciones que han sacado a la luz los programas de espionaje a gran escala que está llevando a cabo el Gobierno de los Estados Unidos, y que también afecta a ciudadanos de la Unión Europea, y ha puesto en la lista de prioridades de la Comisión la regulación en la materia, ya que la regulación actual es *"desigual"* para los ciudadanos comunitarios y los estadounidenses. Sirva como ejemplo que un ciudadano estadounidense que considere violada su privacidad puede reclamar ante las autoridades europeas, mientras un europeo no puede hacer lo mismo frente la administración estadounidense».

[8] http://observatorio.cisde.es/?p=7546 junio 17, 2013 Redacción**. «**Según ha publicado el diario británico «The Guardian» en su página web, el Gobierno del Reino Unido ordenó a sus servicios de inteligencia espiar a los delegados de las cumbres del G-20 en 2009, y también planeaba hacerlo en la cumbre de Commonwealth que se celebró en Trinidad ese mismo año».

Pero libertad, se reitera, no puede significar impunidad. Y ello incluso viene reconocido no solo por los gobiernos y autoridades de los diversos estados, sino incluso por las organizaciones y organismos supranacionales e internacionales como la Unión Europea (UE), el Consejo de Europa, o la ONU. De ello sirve de ejemplo en el marco de la UE, los dictámenes y comunicaciones elaborados sobre los delitos informáticos[9] o sobre la protección de la infancia en Internet, en los que se han expuesto los principios esenciales que respaldan la lucha contra el uso de Internet con fines delictivos o criminales, y en los que aun rechazando la censura, la vigilancia generalizada y los obstáculos a la libertad de expresión y comunicación en la red global se afirma categóricamente que *«la red Internet no está al margen de la ley»*.

En tales términos se han orientado las reformas legislativas, sobre todo las penales, en torno al ámbito económico patrimonial y a la protección de la intimidad y de los datos personales, siendo a este último ámbito al que mayor preponderancia se le ha dado por las legislaciones internas de los Estados miembros de la UE y los del Consejo de Europa, y su consideración como objetivos prioritarios, frente al Derecho anglosajón que ha incidido más en el económico patrimonial.

2. CONCEPTO DE DELITO INFORMÁTICO

Siguiendo el criterio de VELASCO NUÑEZ[10], y teniendo, especialmente, en cuenta su adaptación al objeto de la ponencia utilizaremos un concepto amplio de delitos informáticos, incluyendo tanto el delito tradicional cometido a través de ordenador o Internet (injurias a través de correo electrónico, venta de droga, extorsión o amenazas vehiculizadas a través de Internet, etc.), como el propiamente tal, delito contra la informática —por atacar los datos o sistemas informáticos o las vías telemáticas de comunicación, especialmente a través de Internet—, ya sea bloqueando sistemas (ataques de denegación de servicio o DDoS), destruyendo programas, dañando dispositivos de almacenamiento, alteran-

[9] Así el dictamen del Comité Económico y Social sobre la *«Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre la Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos»* —Europe 2002— (CES 115/2001).

[10] VELASCO NUÑEZ, E., *«Delitos cometidos a través de Internet. Cuestiones Procesales».* La Ley-Actualidad, 2010.

do datos (fraude), destruyéndolos (sabotaje) o usándolos ilícitamente (piratería, espionaje).

Junto a este concepto meramente instrumental, usaremos igualmente el de delitos telemáticos, tratando de agrupar aquellos delitos que en parte o en el todo se desarrollan a través de las nuevas tecnologías.

3. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

3.1. Clasificación tripartita

Para delimitar mejor las conductas incluibles en este concepto tan amplio, que hemos ofrecido, parece adecuado desde el punto de vista expositivo utilizar, la muy extendida clasificación tripartita de los delitos informáticos que se expondrá a continuación:

3.1.1 Ciberdelincuencia económica

Delitos económico-patrimoniales vinculados a la informática.

Se trata de ataques a bienes jurídicos patrimoniales ajenos, vehiculizados a través de la informática, siempre realizados con la intención, por cualquier medio, de consumar apoderamientos o beneficios económicamente evaluables sobre el patrimonio de terceras personas. Constituyen la mayor parte de los delitos informáticos que se denuncian. En nuestro Código Penal principalmente son: el robo inutilizando sistemas de guardia criptográfica, la estafa informática, la defraudación de telecomunicaciones informáticas, el uso no autorizado de terminales informáticos, daños informáticos, estragos informáticos, contra la propiedad intelectual o industrial informática, espionaje informático de secretos de empresa, publicidad engañosa, manipulaciones en aparatos en perjuicio del consumidor, contra el mercado informático, blanqueo informático de capitales y falsedad documental en soporte electrónico.

3.1.2. Ciberdelincuencia intrusiva

Atentados por medios informáticos contra la intimidad y la privacidad: se trata de los ataques al bien jurídico privacidad como un concepto que incluyendo el de intimidad, va más allá, pues abarca todas las modalidades

protegidas en el art. 18 CE (el honor, la intimidad personal, la familiar, la propia imagen, el domicilio, el secreto de las comunicaciones o el uso correcto de la informática).

Suponen una cuarta parte de los delitos que se denuncian y, entre otros, se encuentran tipificados en el Código Penal las amenazas y coacciones informáticas, la distribución de material pornográfico y pornografía infantil, el descubrimiento y revelación de secretos, las injurias y calumnias informáticas y la cesión no consentida de datos ajenos.

3.1.3. Ciberespionaje y Ciberterrorismo

Ataques por medios informáticos contra intereses supraindividuales: se trata de los ataques más graves, que afectan indiscriminadamente a intereses generales de la población, con la intención de crear pánico y terror, para subvertir el sistema político o de convivencia generalmente aceptado.

Apenas tiene incidencia estadística, pero su realización, por afectar a la población en general, genera una alta intranquilidad y desasosiego.

También podríamos incluir dentro de este grupo, conforme a nuestro Código Penal, la usurpación de funciones públicas, la incitación al odio o el descubrimiento y revelación de secretos relativos a la defensa nacional.

3.2. Instrucción 2/2011, de la fiscalía general del estado

Junto a la clasificación expuesta expondremos por su interés, y por ser la que seguiremos al analizar los tipos penales militares incluibles dentro de este concepto, la ofrecida en la 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 al delimitar el marco competencial del Fiscal de Sala coordinador para la criminalidad informática. Esta, meramente instrumental, cuya adopción explica la propia Instrucción[11] es la que

[11] *«Efectivamente junto a tipos penales a través de los cuales el legislador ha protegido específicamente la seguridad de los datos, programas y/o sistemas informáticos, existen otras conductas ilícitas que, afectando a los más diversos bienes jurídicos, se planifican y ejecutan aprovechando las ventajas que ofrecen las nuevas tecnologías de la sociedad de la información y que presentan por tanto, a los efectos de su investigación y/o enjuiciamiento singularidades y dificultades similares a las de los primeramente indicados».* Estas serán incluibles: *«cuando, en los indicados supuestos, la utilización de dichas tecnologías resulte ser determinante en el desarrollo de la actividad delictiva y/o dicha circunstancia implique una elevada complejidad en la dinámica comisiva y, en consecuencia, una mayor dificultad en la investigación del hecho e identificación de sus responsables. Todas estas*

sigue, relacionándola con su calificación jurídica penal en el actual Código Penal, tras las modificaciones operadas por la Ley Orgánica 5/2010, de 22 de junio, que adaptaremos a las introducidas por la Ley Orgánica 1/2015, de 30 de marzo, que tipifica, específicamente, numerosas conductas relacionadas con esta materia:

3.2.1. Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TIC

− Delitos de daños, sabotaje informático y ataques de denegación de servicios previstos y penados en el artículo 264 a 264 quater y concordantes del Código Penal.

− Delitos de acceso sin autorización a datos, programas o sistemas informáticos previstos y penados en el artículo 197 bis del Código Penal.

− Delitos de descubrimiento y revelación de secretos del artículo 197 del Código Penal cometidos a través de las TIC o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos.

− Delitos de descubrimiento y revelación de secretos de empresa previstos y penados en el artículo 278 del Código Penal cometidos a través de las TIC o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos o electrónicos.

− Delitos contra los servicios de radiodifusión e interactivos previstos y penados en el artículo 286 del Código Penal.

3.2.2. Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TIC

− Delitos de estafa previstos y penados en el artículo 248.2 a) b) y c) del Código Penal, siempre que, en los supuestos a) y c) se utilicen las TIC para llevar a efecto la transferencia u operación de cualquier tipo en perjuicio de otro.

---

circunstancias determinan que el catálogo inicial de delitos a los que se extiende el marco competencial del área de criminalidad informática… quede necesariamente abierto a la posibilidad de hacerse extensivo a otras conductas cuando concurran las circunstancias antedichas que deberán ser analizadas en el momento oportuno». 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.

− Delitos de acoso a menores de 13 años, «*child grooming*», previstos y penados en el artículo 183 bis a 183 quater del Código Penal cuando se lleve a efecto a través de las TIC.

− Delitos de corrupción de menores o de personas discapacitadas o relativas a pornografía infantil o referida a personas discapacitadas previstos y penados en el artículo 189 del Código Penal cuando para el desarrollo y/o ejecución de la actividad delictiva se utilicen las TIC.

− Delitos contra la propiedad intelectual de los artículos 270 y ss. del Código Penal cuando se cometan utilizando las TIC.

3.2.3. Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TIC, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia

− Delitos de falsificación documental de los artículos 390 y ss. del Código Penal cuando para la ejecución del delito se hubieran empleado las TIC siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad técnica en la investigación criminal.

− Delitos de injurias y calumnias contra funcionario público, autoridad o agente de la misma previstos y penados en los artículos 205 y ss. del Código Penal cometidos a través de las TIC siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

− Delitos de amenazas y coacciones previstos y penados en los artículos 169 y ss. del Código Penal cometidos a través de las TIC siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

− Delitos contra la integridad moral previstos y penados en el artículo 173.1 del Código Penal cometidos a través de las TIC siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

− Delitos de apología o incitación a la discriminación, el odio y la violencia o de negación o justificación de los delitos de genocidio previstos y penados en los artículos 510 y 510 bis del Código Penal cometidos a través de las TIC siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

− Cualquier otro tipo delictivo en cuya ejecución haya sido determinante la utilización de las TIC y en los que dicha circunstancia genere una especial complejidad en la investigación criminal.

4. LA ESPECIALIZACIÓN: REQUISITO PREVIO

El primer rasgo que destaca al afrontar los problemas que plantea la delincuencia informática es la necesidad de poseer un conocimiento especializado para llevar a buen término su investigación. En el ámbito del derecho procesal y de la obtención de pruebas de la comisión de delitos, no solo los delitos informáticos *stricto sensu* se persiguen investigando en dicho entorno, sino que muchos otros delitos también pueden dejar rastros o pruebas en el entorno electrónico, telemático o virtual. Y para realizar investigaciones con fines penales en un entorno electrónico, son necesarios conocimientos técnicos especializados, procedimientos adecuados y facultades legales suficientes.

Muchos Estados, entre ellos el nuestro, han creado departamentos policiales especializados en delincuencia informática —tanto el Cuerpo de Policía Nacional, como la Guardia Civil, entre otros, cuentan con ellos[12]— y fiscales especializados en delitos informáticos, como hemos visto. Incluso, en algunos países, se han preparado diversos manuales con instrucciones técnicas, forenses y de procedimiento sobre la manera de llevar a cabo una investigación para reducir la pérdida de pruebas y garantizar la admisibilidad de estas ante los tribunales.

Algunos departamentos policiales nacionales *«patrullan»* por Internet, y se han creado programas informáticos específicos para detectar delitos como 1a piratería informática o la distribución de pornografía infantil, y, dado el enorme volumen de información que contienen las redes telemáticas internacionales, parece indispensable elaborar este tipo de programas informáticos.

Las peculiaridades que más se han puesto de manifiesto, con la progresiva utilización de Internet, desde el punto de vista del ámbito de la prueba, acrecentando consecuentemente la peculiaridad de dificultad en su averiguación y descubrimiento son, en primer lugar, no solo el carácter intangible de los datos y de la información que contienen, sino el carácter

[12] Brigada de Investigación Tecnológica de Cuerpo Nacional de Policía, Equipo de Investigación Tecnológica de la Guardia Civil y Unidad de Delitos Informáticos de Mossos d'Esquadra.

eminentemente volátil de los mismos al contenerse en un espacio virtual y en un sistema de continua transferencia y transmisión que permite su supresión, alteración, transformación u ocultación en cualquier momento, con serias dificultades incluso para lograr su conservación o almacenamiento en un soporte, no ya documental ordinario, sino al menos electromagnético. Pero es que aún en este caso, la sencilla falta de visualización de los datos almacenados electromagnéticamente ya dificulta de forma considerable la acreditación del ilícito, pues cualquiera que quisiera comprobarlos y revisarlos, no puede hacerlo directamente sobre los datos que le interesan, sino que siempre debe acudir a los términos del ordenador y a las comunicaciones a través de la pantalla, que, además, pueden haber sido objeto de manipulación.

Además, el distanciamiento temporal y espacial. Internet ha acrecentado el grado de posibilidad de separación temporal entre la comisión de la inicial acción ilícita por el sujeto activo y su materialización final con la obtención del resultado o los efectos perjudiciales o lesivos de la misma. Por otro lado, la característica del distanciamiento espacial, esto es, el que el sujeto se encuentre físicamente distante no solo del lugar donde se materializan los efectos de su comportamiento ilícito, sino incluso de aquel, en donde se encuentra el equipo o terminal informática, desde el que se *«lanza»* o materializa la acción ilícita, o el servidor que da el acceso a la red a tal acción realizada por el equipo o terminal a instrucción del sujeto activo responsable material. Y todo ello ha dado lugar a serios conflictos competenciales.

5. PRINCIPAL NORMATIVA EN LA MATERÍA

5.1. El convenio sobre ciberdelincuencia del Consejo de Europa

Los diversos gobiernos nacionales y organismos internacionales trabajan en diversos ámbitos dirigidos a obtener tratados y convenios globales sobre los delitos informáticos. Como exponente más importante de esta tarea cabe destacar en el marco del Consejo de Europa, el *Convenio sobre la Ciberdelincuencia* del Consejo de Europa*,* suscrito, a fecha de hoy, por 47 Estados, algunos de ellos como EE. UU., Canadá, la República de Sudáfrica, Australia o Japón, no pertenecientes al Consejo de Europa, y abierto a su ratificación en Budapest, Hungría, el 23 de noviembre de 2001. Dicho Convenio que entró en vigor para España, tras su ratificación, el 10 de octubre de 2010, constituye un hito en la lucha coordinada y eficaz contra este tipo de conductas. Siendo el primer instrumento multilateral dirigido a sentar las

bases para afrontar los problemas planteados por la expansión de la actividad criminal en las redes informáticas y telemáticas.

Con carácter general, hemos de hacer las siguientes precisiones:

5.1.1. En el **ámbito de la prueba** partiendo de la base de que la investigación de la cibercriminalidad se lleva a cabo en un medio particularmente volátil, ya el primer título, dedicado a las disposiciones generales, en su artículo 14, al referirse al alcance de las disposiciones procesales, sostiene en su apartado 2, c, la obligación para cada parte de adoptar las medidas necesarias, incluso legislativas, para regular la obtención de pruebas en forma electrónica de un ilícito penal. Y el artículo 15, prevé las condiciones y reservas a efectuar en este ámbito procesal por los Estados firmantes a tenor de sus respectivas legislaciones internas en orden a preservar y respetar los derechos humanos y las libertades fundamentales, así como el principio de proporcionalidad.

5.1.2. La intención del Convenio es **adaptar las medidas procesales tradicionales**, como el registro y comiso, al nuevo medio tecnológico de la telemática, si bien crea nuevas medidas como la inmediata conservación de datos, en orden a asegurar las tradicionales medidas de almacenamiento, o el registro y comiso de datos, de modo que permanezcan efectivos en este ambiente eminentemente volátil. Reconociendo incluso que los datos en el ámbito de las nuevas tecnologías, informática y telemática, no son siempre elementos estáticos, sino que fluyen en el proceso de la comunicación, el Convenio adapta a tal finalidad otros procedimientos tradicionales de obtención de pruebas en las telecomunicaciones, como la obtención e interceptación en tiempo real de datos de tráfico o de contenido. Y todo ello con la finalidad de permitir la obtención o almacenamiento de datos en una investigación o procedimiento criminal. Claro está que en todos los artículos de esta Sección, viene de continuo la referencia a *«las autoridades competentes y poderes»* el que deban garantizar las medidas y procedimientos señalados para fines de investigaciones y procedimientos específicamente criminales. Y como en muchos países del Consejo de Europa solo los órganos judiciales tienen la facultad de ordenar o autorizar el almacenamiento o creación de pruebas, mientras que en otros tal capacidad o facultad les viene concedida asimismo a los Fiscales o a autoridades gubernativas, incluso administrativas, tal término conceptual comprende a toda aquella autoridad que por su legislación nacional tiene la capacidad de ordenar, autorizar o acordar la ejecución de medidas procesales de ob-

tención, almacenamiento y creación de pruebas en el marco de investigaciones o procedimientos específicamente criminales.

5.2. El código penal

Las reformas más importantes, en lo que nos afecta, han sido las modificaciones del **Código Pena**l, introducidas por la Ley Orgánica 5/2010, de 22 de junio, y por la Ley Orgánica 1/2015, de 30 de marzo, que tipifican específicamente, determinadas conductas relacionadas con la materia a las que ya hemos hecho referencia anteriormente y que sintetizaremos en las siguiente clasificación:

5.2.1. *Ciberdelincuencia económica*

Art. 238.5 CP. Robo inutilizando sistemas de guardia criptográfica.

Art. 248.2 CP. Estafa informática, en su doble modalidad de:

- Estafa por ingeniería social: a través del engaño a personas (*phising*, cartas nigerianas, estafas de ONG, timo del Gordo, ventas de segunda mano, falsas subasta e-Bay, etc.).
- Estafa por ingeniería informática: a través de manipulación informática o artificio semejante.

Art. 255 CP. Defraudación de telecomunicaciones informáticas.

Art. 256 CP. Hurto de tiempo informático, o uso no autorizado de terminales informáticos.

Arts. 264 y ss. CP. Virus o daños informáticos, cuando se produce sobre datos. Cuando los daños persiguen a los sistemas informáticos (no a los datos en sí mismo) estamos ante un *sabotaje informático* que se castiga, también, como delito de estragos, art. 346 CP, o si fuera con intencionalidad terrorista, mediante el art. 571 CP.

Art. 270.3 CP. Contra la propiedad intelectual informática, en cualquiera de sus modalidades creativas (protección penal de los derechos de autor) y 271 CP.

Arts. 273 a 276 CP. Contra la propiedad industrial, con protección penal.

Arts. 278 a 280 CP. Espionaje informático de secretos de empresa.

Art. 282 CP. Publicidad engañosa.

Art. 283 CP. Manipulaciones en aparatos en perjuicio del consumidor.

Art. 286 CP. Contra el mercado informático.

Art. 298 CP. Receptación de cableado, equipos o componentes… de servicios de telecomunicaciones.

Art. 301 CP. Blanqueo informático de capitales.

Art. 390 CP. Falsedad documental, cuando el soporte sea de naturaleza informática.

5.2.2. *Ciberdelincuencia intrusiva*

Arts. 169 y 172 CP. Amenazas y coacciones informáticas.

Art. 183 ter. CP. Utilizar internet, teléfono o de cualquier otra tecnología de la información y la comunicación para contactar con un menor a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189 o realizar actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor.

Arts. 186 a 189 CP. Distribución de material pornográfico y pornografía infantil.

Arts. 197 a 200 CP. Descubrimiento y revelación de secretos, que es el delito informático intrusivo por excelencia.

Arts. 205 a 216 CP. Injurias y calumnias informáticas, con el art. 211 que las reputa hechas con publicidad en atención al medio por el que se propagan.

Arts. 417, 418 y 423 CP. Cesión no consentida de datos ajenos, a través de la infidelidad en la custodia de documentos y violación de secretos para su venta, hecha por empleado público, que la tiene funcionalmente prohibida.

5.2.3. *Ciberterrorismo y Ciberespionaje*

Art. 402 CP. Usurpación de funciones públicas mediante correo electrónico.

Arts. 598 y 603 CP. Descubrimiento y revelación de secretos relativos a la defensa nacional.

5.3. Ley 25/2007, de *«conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones»*

La ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, articulándolo a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de esta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

Enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet[13], e incluye dentro de su ámbito de aplicación los datos necesarios para identificar el origen y

---

[13] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Artículo 3 *Datos objeto de conservación*

1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:
- i) Número de teléfono de llamada.
- ii) Nombre y dirección del abonado o usuario registrado.

2.º Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:
- i) La identificación de usuario asignada.
- ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.
- iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:
- i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.
- ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:
- i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.
- ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

destino de la comunicación, así como la identidad de los usuarios o abonados de ambos (nombre y dirección), los que permiten determinar el mo-

---

1.º Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.

2.º Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.

ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).

2.º Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.

2.º Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.

ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.

iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.

iv) La IMSI de la parte que recibe la llamada.

v) La IMEI de la parte que recibe la llamada.

vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.º Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.º La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2.º Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta ley.

mento y duración, el tipo de servicio y el equipo de comunicación utilizado por los usuarios que, cuando se trate de un equipo móvil, también abarcará los datos necesarios para su localización. Todos estos datos deberán conservarse doce meses, computados desde la fecha en la que se produjo la comunicación, no pudiéndose conservar ningún otro que pudiera revelar el contenido de la misma.

En todo caso, la cesión de tales datos por las operadoras se subordina conforme al art. 1.1 de la ley a «*la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales».* En definitiva, con el marco jurídico vigente, toda investigación policial o del Ministerio Fiscal para el esclarecimiento de un hecho delictivo que requiera la cesión de alguno de los datos almacenados por las operadoras necesitará autorización del Juez de Instrucción[14].

5.4. Ley orgánica 13/2015, de *«modificación de la ley de enjuiciamiento criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica»*

Constituye un hito en la regulación procesal de la materia pues como explica en su exposición de motivos: «*La Ley de Enjuiciamiento Criminal no ha podido sustraerse al paso del tiempo. Renovadas formas de delincuencia ligadas al uso de las nuevas tecnologías han puesto de manifiesto la insuficiencia de un cuadro normativo concebido para tiempos bien distintos. Los flujos de información generados por los sistemas de comunicación telemática advierten de las posibilidades que se hallan al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos. Surge así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros».*

Los principios en que se basa la reforma aparecen recogidos en el nuevo artículo 588 bis a. *«**Principios rectores**. 1. Durante la instrucción de las*

[14] Acuerdo del Pleno no jurisdiccional de la Sala 2.ª del Tribunal Supremo de 23 de febrero de 2010 «*es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo»*. Así, el Ministerio Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007, de 18 de octubre.

causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de ***especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida****. 2. El principio de* ***especialidad*** *exige que una medida esté relacionada con la investigación de un delito concreto… 3. El principio de* ***idoneidad*** *servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad. 4. En aplicación de los principios de* ***excepcionalidad y necesidad*** *solo podrá acordarse la medida: a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida. 5. Las medidas de investigación reguladas en este capítulo solo se reputarán* ***proporcionadas*** *cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho».*

La ley establece en materia de *intervención de comunicaciones telefónicas y telemáticas* un criterio más amplio que el antes expuesto, así dispone, en su artículo 588 ter. a. *«****Presupuestos****. La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1*[15] *de esta ley o* ***delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación****»*. Enumeración basada, principalmente, en el medio empleado para la comisión del delito, que, a nuestro juicio, deberemos conjugar, a la hora de aplicarla con los *principios rectores* enunciados en el artículo 588 bis a., recogidos en el párrafo precedente.

[15] «Artículo 579. … 1.º Delitos dolosos castigados con **pena con límite máximo de, al menos, tres años de prisión**. 2.º Delitos cometidos en el seno de un **grupo u organización criminal**. 3.º Delitos de **terrorismo**».

Respecto a la incorporación al proceso de los *datos electrónicos de tráfico o asociados***,** la reforma acoge el criterio fijado por la Ley 25/2007, exigencia de autorización judicial para su cesión, su incorporación al proceso solo se autoriza cuando se trate de la investigación de un delito que, por razones vinculadas al principio de proporcionalidad, sea de los que justifican el sacrificio de la inviolabilidad de las comunicaciones. Se da un tratamiento jurídico individualizado al acceso por agentes de policía al IMSI, IMEI, dirección IP y otros elementos de identificación de una determinada tarjeta o terminal, en consonancia con la jurisprudencia del Tribunal Supremo. También se regula el supuesto de la cesión de datos desvinculados de los procesos de comunicación concernientes a la titularidad o identificación de un dispositivo electrónico, a los que podrá acceder el Ministerio Fiscal o la Policía Judicial en el ejercicio de sus funciones sin necesidad de autorización judicial.

Establece, asimismo, la citada ley en su artículo 588 ter. e.) el denominado *«**Deber de colaboración**. 1. Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones. 2. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades. 3. Los sujetos obligados que incumplieren los anteriores deberes podrán incurrir en delito de desobediencia».*

Por último, señalar que la ley introduce, una pluralidad de medios de investigación, entre ellos el agente encubierto informático[16], o el registro remoto sobre equipos informáticos que facilitaran, notablemente, la investigación de los delitos cometidos mediante el uso de las TIC, regulando, asimismo, los requisitos materiales y formales que les son de aplicación.

[16] De una parte se prevé la posibilidad de que los agentes encubiertos puedan obtener imágenes y grabar conversaciones, siempre que recaben específicamente una autorización judicial para ello; y de otra, se regula la figura del agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación (puesto que en los canales abiertos, por su propia naturaleza, no es necesaria) y que a su vez, requerirá una autorización especial para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación.

6. EL CÓDIGO PENAL MILITAR DE 2015

La Ley Orgánica 15/2015, de 14 de octubre, del Código Penal Militar (en adelante CPM), entró en vigor el 15 de enero de 2016, conforme establece su disposición final octava. A diferencia de su predecesor, CPM 1985, recoge delitos, genuinamente, informáticos, principalmente, mediante remisión a su regulación en el Código Penal (*delitos en los que el objeto de la* ***actividad delictiva son los propios sistemas informáticos o las TIC)***. Junto a ellos, nos encontraremos, siguiendo el criterio amplio que hemos adoptado (el contenido en la Instrucción de la Fiscalía General del Estado 2/2011), que habrán de incluirse:

− *aquellos en los que la actividad criminal* ***se sirve para su ejecución de las ventajas que ofrecen las TIC****.;*

− *aquellos en los que la actividad criminal,* ***además de servirse para su ejecución de las ventajas que ofrecen las TIC, entraña especial complejidad en su investigación que demanda conocimientos específicos*** *en la materia;*

− *cualquier otro tipo delictivo en* ***cuya ejecución haya sido determinante la utilización de las TIC*** *y en los que dicha circunstancia genere una* ***especial complejidad en la investigación criminal***.

Examinaremos algunas de las conductas descritas en los tipos contenidos en el CPM, para delimitar si cumplirían alguno de los criterios adelantados, a fin de incluirlos dentro de la categoría de delitos informáticos, así:

6.1. Tipos penales más relevantes

Con arreglo a la experiencia acumulada, en la aplicación del antiguo CPM, el núcleo fundamental de delitos cometidos a través de las TIC en el ámbito de la Jurisdicción Militar se centraría en los siguientes preceptos:

6.1.1. *Atentados contra los medios o recursos de la Seguridad o Defensa Nacionales*

Dentro del ***TÍTULO I. Delitos contra la seguridad y defensa nacionales***

Artículo 27

El militar *que, con el propósito de atentar contra los medios o recursos de la seguridad o defensa nacionales, cometiere alguno de*

*los delitos previstos en los **artículos 264 a 266** del Código Penal será castigado con la pena de ocho a veinticinco años. la misma pena se impondrá al que cometiere este delito en situación de conflicto armado o estado de sitio, cuando no tenga la condición militar.*

Las conductas que aparecen citadas en dichos preceptos, del Código Penal, son, entre otras: los delitos de **daños, sabotaje informático y ataques de denegación de servicios** previstos y penados en los artículos 264, 264 bis y 264 ter, que contendrían los siguientes supuestos:

Borrado, daño, deterioro, alteración, supresión o hacer inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, con o sin afección al sistema informático de una infraestructura crítica o 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.

O, sin estar debidamente autorizado, obstaculizar o interrumpir 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.

O, producir, adquirir para su uso, importar o, de cualquier modo, facilitar a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores: a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Quedará excluida la aplicación del Código Penal Militar a los supuestos contenidos en el artículo 264 quater, al no ser aplicable, en esencia, a la persona jurídica responsable la condición de *«militar»*, que exige para el autor el artículo 27 CPM.

Tampoco, serán aplicables los preceptos castrenses, en el caso de que no hallemos ante un delito de terrorismo del artículo 573 del Código Penal[17].

[17] ***Artículo 573.*** *1. Se considerarán 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*

6.1.2 *Espionaje y revelación secretos o informaciones relativas a la Seguridad Nacional o Defensa Nacional*

Incluiremos aquí los contenidos en el artículo 26 CPM.

*«**El militar** que cometiere **cualquiera de los delitos previstos en los artículos 277 ó 598 a 603 del Código Penal** será castigado con la pena superior en grado a la establecida en el mismo. En situación de conflicto armado o estado de sitio se impondrá la pena superior en uno o dos grados.*

*Si estos delitos se cometieren **en situación de conflicto armado o estado de sitio por quien no tenga la condición militar**, se castigarán con la pena superior en grado a la prevista en el Código Penal».*

La referencia comprende los siguientes artículos:

Artículo 277

*Será castigado… el que **intencionadamente haya divulgado la invención objeto de una solicitud de patente secreta, en contravención con lo dispuesto en la legislación de patentes, siempre que ello sea en perjuicio de la defensa nacional**.*

Del descubrimiento y revelación de secretos e informaciones relativas a la defensa nacional

Artículo 598

*El que, **sin propósito de favorecer a una potencia extranjera, se procurare, revelare, falseare o inutilizare información legalmente calificada como reservada o secreta, relacionada con la seguridad***

---

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, cuando se llevaran a cabo con cualquiera de las siguientes 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.

*2. Se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y **264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterio**r …*

nacional o la defensa nacional o relativa a los medios técnicos o sistemas empleados por las Fuerzas Armadas o las industrias de interés militar*…*

Artículo 599

La pena establecida en el artículo anterior se aplicará en su mitad superior cuando concurra alguna de las circunstancias siguientes:

1.º Que el sujeto activo sea depositario o conocedor del secreto o información por razón de su cargo o destino.

2.º Que la revelación consistiera en dar publicidad al secreto o información en algún medio de comunicación social o de forma que asegure su difusión.

Artículo 600

1.º El que ***sin autorización expresa reprodujere planos o documentación referentes a zonas, instalaciones o materiales militares que sean de acceso restringido y cuyo conocimiento esté protegido y reservado por una información legalmente calificada como reservada o secreta****…*

2.º …el que ***tenga en su poder objetos o información legalmente calificada como reservada o secreta, relativos a la seguridad o a la defensa nacional****, sin cumplir las disposiciones establecidas en la legislación vigente.*

Artículo 601

El que, ***por razón de su cargo, comisión o servicio, tenga en su poder o conozca oficialmente objetos o información legalmente calificada como reservada o secreta o de interés militar, relativos a la seguridad nacional o la defensa nacional, y por imprudencia grave dé lugar a que sean conocidos por persona no autorizada o divulgados, publicados o inutilizados****…*

Artículo 602

El que ***descubriere, violare, revelare, sustrajere o utilizare información legalmente calificada como reservada o secreta relacionada con la energía nuclear****….*

Artículo 603

El que ***destruyere, inutilizare, falseare o abriere sin autorización la correspondencia o documentación legalmente calificada como reservada o secreta, relacionadas con la defensa nacional y que tenga en su poder por razones de su cargo o dest****ino...*

Los preceptos citados, cuyo contenido es más amplio que el que recogían los artículos 53 a 56 y 116 del CPM 1985, dan protección a información clasificada, relativa a la seguridad nacional o defensa nacional, lo que nos conduce a la normativa que regula los secretos oficiales, Ley 9/1968, de 5 de abril, reguladora de los secretos oficiales, modificada por Ley 48/1978, de 7 de octubre y su Reglamento aprobado por Decreto 242/1969, de 20 de febrero. Cuya anunciada reforma no termina de llegar, pese a su inadaptación al momento actual.

En el ámbito del Ministerio de Defensa es importante hacer referencia a la hora de determinar la gravedad de las conductas a las normas sobre materias clasificadas, bien jurídico protegido por los preceptos indicado. En efecto; de acuerdo con la normativa actualmente vigente en esta materia, concretamente el apartado sexto, punto 4, del texto por el que se regula la vigente Política de Seguridad de la Información del Ministerio de Defensa, aprobado por Orden Ministerial 76/2006, de 19 de julio, y desarrollado por la Instrucción 41/2010, de 7 de julio, del secretario de Estado de Defensa, cabe distinguir entre los documentos militares: clasificados y los no clasificados. Respecto a los primeros, existen cuatro grados de clasificación: *1) SECRETO, 2) RESERVADO, 3) CONFIDENCIAL y 4) DIFUSIÓN LIMITADA*. Los numerados 1) y 2), para «materias clasificadas» en sentido estricto, cuyo conocimiento por personas no autorizadas pueden dañar o poner en riesgo la seguridad y defensa del Estado; y los grados 3) y 4), referidos «materias objeto de reserva interna», cuyo conocimiento por personas no autorizadas pudiera afectar a la seguridad del Ministerio de Defensa, amenazar sus intereses o dificultar el cumplimiento de su misión. Por su parte, la información no clasificada puede ser dividida, dependiendo de su ámbito de distribución, en dos categorías: 1) Información de *USO OFICIAL*, cuya distribución está limitada al ámbito del Ministerio de Defensa, o a personas u organismos que desempeñen actividades relacionadas con el mismo; y 2) información de *USO PÚBLICO*, cuya distribución no está limitada.

La «*Información de USO OFICIAL»*, si bien es cierto que no está «clasificada» y no lleva sello, marca o distintivo alguno, puesto que solo la clasificada lo lleva, no puede al no tratarse de *«Información de USO PÚBLICO»*, ser difundido de manera indiscriminada en una

web abierta en la que cualquier individuo puede entrar desde un ordenador portátil en cualquier parte del mundo y navegar libremente por ella (otra cosa, como es lógico, es la utilización de MESINCET a través de la red INTRANET de los Cuarteles Generales o del propio Ministerio de Defensa, solo accesible a través de ordenadores enlazados mediante servidor oficial y con las debidas restricciones y controles de seguridad: identificación con IP y contraseña de cada usuario autorizado, entre otras). Dice a este respecto la Orden Ministerial, anteriormente citada, en su apartado séptimo, punto 1, que *«para el acceso a información clasificada de DIFUSIÓN LIMITADA o inferior [que es el supuesto de la no clasificada], no se requerirá habilitación personal de seguridad específica. Se permitirá el acceso cuando "la persona sea conocedora de sus responsabilidades, y tenga necesidad de conocer dicha información para el desempeño de sus cometidos oficiales»*[18].

La exigencia de la obligada discreción aparece reforzada por la Ley Orgánica 9/2011, de 27 de julio*, «de derechos y deberes de los miembros de las Fuerzas Armadas»,* que se ocupa en su artículo 21 del «*Deber de reserva»*, estableciendo que:

> *«1. El militar está sujeto a la legislación general sobre secretos oficiales y materias clasificadas.*
>
> *2. Guardará la debida discreción sobre hechos o datos no clasificados relativos al servicio de los que haya tenido conocimiento por su cargo o función, sin que pueda difundirlos por ningún medio ni hacer uso de la información obtenida para beneficio propio o de terceros o en perjuicio del interés público, especialmente de las Fuerzas Armadas».*

[18] Auto de fecha 7 de septiembre de 2010, del Juzgado Togado Central n.º1 en Diligencias Previas 1/05/10, que acuerda el archivo de las actuaciones *«En definitiva, el documento en cuestión no debió nunca ser volcado en una web pública, ni siquiera de una Asociación de Suboficiales cuyos miembros, como profesionales de la milicia, pudieran justificar su interés por conocer los informes, escritos, notas o documentos que allí se contienen, puesto que tal Asociación privada no está, como entidad con personalidad jurídica propia, entre los destinatarios del "Mensaje de FUTER" ni consta que haya solicitado y obtenido de la autoridad competente. La Asociación de Suboficiales de las Fuerzas Armadas debió comprobar previamente y pudo haberlo hecho sin más dificultad que preguntárselo a FUTER directamente, tampoco aparece que el presunto error, negligencia o ligereza que supuso tal difusión, ni en la persona desconocida que dio traslado del documento a ASFAS ni en aquélla que volcó tal documento en la página, web, posiblemente sin malicia ni intención espuria sino por creer honestamente que se trataba de información "inocua" al no estar clasificada, posea entidad suficiente para ser considerado constitutivo de ilícito penal».*

6.1.3. *Delitos contra la disciplina*

El primero que hemos de examinar es el delito de **sedición militar** tipificado en el:

Artículo 38 CPM

*«Los militares que, **mediante concierto expreso o tácito**, en número de cuatro o más o que, sin llegar a este número, constituyan al menos la mitad de una fuerza, dotación o tripulación, se negaren a obedecer o no cumplieren las órdenes legítimas recibidas, incumplieren los demás deberes del servicio o amenazaren, ofendieren o ultrajaren a un superior…».*

Artículo 39 CPM

Segundo párrafo *«Las demás reclamaciones o peticiones colectivas, así como las **reuniones clandestinas** para ocuparse de asuntos del servicio, si pusieran en grave riesgo el mantenimiento de la disciplina, serán castigadas con la pena de tres meses y un día a seis meses de prisión; pudiendo, en otro caso, sancionarse en vía disciplinaria militar».*

Artículo 40 CPM

*«2. La **provocación, la conspiración y la proposición** para la ejecución de los delitos previstos en este Capítulo se castigarán con la pena inferior en uno o dos grados a la que correspondería a los mismos».*

Las TIC posibilitan la realización de algunas de las conductas tipificadas, favoreciendo la ocultación de la identidad de los proponentes, o mediante la utilización del correo electrónico, en forma anónima o inidentificada o procedimientos similares[19].

Aunque el texto típico parece exigir la presencia corpórea, no es descartable que para llegar a alcanzar el *concierto expreso o tácito* o para la celebración de las *reuniones clandestinas* a que se refieren los artículos 38 y 39 CPM, se puedan hacer uso de las TIC, ya sea mediante mensajería o transmisiones «on line» o por, algún otro sistema de comunicación interactiva, como la videoconferencia.

Dentro de los **delitos de Insubordinación**, abordaremos en primer lugar el delito de insulto a superior.

[19] Diligencias Previas 25/06/13, incoadas con fecha 26 de abril de 2013 contra autores desconocidos en averiguación de la posible comisión de un delito de sedición.

Artículo 43 CPM

«El militar que, sin incurrir en los delitos previstos en el artículo anterior, ***coaccionare, amenazare, calumniare o injuriare gravemente a un superior (…), por escrito o con publicidad****...».*

Es, sin duda, la de más frecuente comisión, de las conductas examinadas, y reviste multitud de variantes. Existe una extensa Jurisprudencia, tanto en la Jurisdicción Militar como en la Ordinaria, sobre la materia. El principal problema que plantea es la determinación última del autor material final de la conducta delictiva, sobre todo, cuando se trata de una terminal particular compartida o un cibercafé unido a la dificultad de investigación que implica su escasa penalidad.

El delito de **abuso de autoridad** aparece tipificado en el:

Artículo 45 CPM

El superior que, ***abusando de sus facultades de mando o de su posición en el servicio, irrogare un perjuicio grave a un subordinado****, le obligare a prestaciones ajenas al interés del servicio o le impidiere arbitrariamente el ejercicio de algún derecho…*

Artículo 47 CPM

El superior que ***tratare a un subordinado de manera degradante, inhumana o humillante****, o realizare actos de agresión o abuso sexuales, será castigado con la pena de seis meses a cinco años de prisión, pudiendo imponerse, además, la pena de pérdida de empleo, sin perjuicio de las que correspondan por los resultados lesivos producidos o las agresiones y otros atentados contra la libertad o indemnidad sexuales efectivamente cometidos, conforme al Código Penal.*

Artículo 48 CPM

El superior que, respecto de un subordinado, realizare ***actos de acoso tanto sexual y por razón de sexo como profesional, le amenazare, coaccionare, injuriare o calumniare, atentare de modo grave contra su intimidad, dignidad personal o en el trabajo, o realizare actos que supongan discriminación grave por razón de nacimiento, origen racial o étnico, sexo, orientación sexual, religión, convicciones, opinión, discapacidad o cualquier otra condición o circunstancia personal o social****…*

Incluiremos junto a ellos por razones de oportunidad los tipos contenidos en los artículos:

Delitos relativos al ejercicio de los derechos fundamentales y de las libertades públicas por los militares

Artículo 49 CPM

*El militar que, sin incurrir en los delitos de insulto a superior o abuso de autoridad**, públicamente, en lugares afectos a las Fuerzas Armadas o a la Guardia Civil o en acto de servicio, maltratare de obra a otro militar, le tratare de manera degradante, inhumana o humillante**, o realizare actos de agresión o de abuso sexuales…*

Artículo 50 CPM

*El militar que, sin incurrir en los delitos de insulto a superior o abuso de autoridad, **públicamente, en lugares afectos a las Fuerzas Armadas o a la Guardia Civil o en acto de servicio, impidiere o limitare arbitrariamente a otro militar el ejercicio de los derechos fundamentales o libertades públicas, realizare actos de acoso tanto sexual y por razón de sexo como profesional, le amenazare o coaccionare, le injuriare gravemente o le calumniare, atentare de modo grave contra su intimidad, dignidad personal o en el trabajo, realizara actos que supongan grave discriminación por razón de nacimiento, origen racial o étnico, sexo, orientación sexual, religión, convicciones, opinión, discapacidad o cualquier otra condición o circunstancia personal o social**…*

Artículo 65 CPM

*1. **El militar que en el ejercicio del mando se excediere arbitrariamente de sus facultades o, prevaliéndose de su empleo, cargo o destino, cometiere cualquier otro abuso grave** será castigado con la pena de tres meses y un día a dos años de prisión. Si empleare u ordenare ejercer contra cualquier persona violencias innecesarias u ordenare, permitiere o hiciere uso ilícito de las armas, será castigado con la pena de cuatro meses a cuatro años de prisión. Todo ello sin perjuicio, en su caso, de la pena que corresponda por los resultados lesivos producidos, conforme al Código Penal.*

Junto al contenido en el artículo 43 CPM, constituye el núcleo fundamental de la delincuencia cometida mediante TIC en la Jurisdicción militar. Vivimos en un momento en que, en pro de la seguridad pública colectiva, se ha comenzado a instalar numerosos sistemas digitales de almacenamiento de datos que, como ya hemos expuesto, merman de forma importante la privacidad de los ciudadanos. Ello también ocurre, en el ámbito del Ministerio de Defensa y, el CPM, abre la vía al castigo de las conductas intrusivas o dañosas realizadas mediante las TIC, susceptibles de ser incluidas en los tipos descritos en los artículos 45 o 65 CPM, dentro de las que cabe incluir las posibles intromisiones que se pueden hacer a la intimidad de los militares, por vía de acceso ilegítimo a sus datos informáticos, cuya protección resulta de la Ley Orgánica 9/2011, de 27 de julio*, «de derechos y deberes de los miembros de las Fuerzas Armadas»,* que se ocupa en su artículo 10. Del «*Derecho a la intimidad y dignidad personal».*

«1. El militar tiene derecho a la intimidad personal. En el ejercicio y salvaguarda de este derecho se tendrán en cuenta las circunstancias en que tengan lugar las operaciones.

También tiene derecho al secreto de las comunicaciones y a la inviolabilidad del domicilio, incluido el ubicado dentro de unidades, en los términos establecidos en la Constitución y en el resto del ordenamiento jurídico.

Se deberá respetar la dignidad personal y en el trabajo de todo militar, especialmente frente al acoso, tanto sexual y por razón de sexo como profesional.

2. Las revistas e inspecciones deberán respetar en todo caso los derechos contenidos en el apartado anterior.

Como norma general, el registro personal de los militares, de sus taquillas, efectos y pertenencias que estuvieren en la unidad requerirá del consentimiento del afectado o resolución judicial. No obstante, cuando existan indicios de la comisión de un hecho delictivo o por razones fundadas de salud pública o de seguridad, el jefe de la unidad podrá autorizar tales registros de forma proporcionada y expresamente motivada. Estos registros se realizarán con la asistencia del interesado y en presencia de al menos dos testigos o sólo de éstos, si el interesado debidamente notificado no asistiera.

3. Los datos relativos a los miembros de las Fuerzas Armadas estarán sujetos a la legislación sobre protección de datos de carácter personal. A tal efecto los poderes públicos llevarán a cabo las accio-

nes necesarias para la plena efectividad de este derecho fundamental, especialmente cuando concurran circunstancias que pudieran incidir en la seguridad de los militares».

La falta de tipos específicos, no es óbice para que diversos tipos del CPM, en los que se castiga el abuso de autoridad, puedan ser utilizados para castigar al superior que accediese, de forma ilegítima, a los datos informáticos privados de un subordinado, o en el ámbito de la Unidad, mediante emails, chats u otros medios de comunicación de carácter público o restringido (por ejemplo grupos de WhatsApp) realizara alguno de los comportamientos descritos, pues esta agresión a su intimidad, podría ser calificada, dependiendo del supuesto de hecho, como delito relativo al ejercicio de los derechos fundamentales y de las libertades públicas por los militares, artículos 49 y 50 CPM, o conforme a los tipos contenidos en los artículos 45 a 48 CPM, siempre y cuando dada la relación entre superior y subordinado, la conexión de los hechos con el servicio y la finalidad perseguida con la intromisión, fuera posible determinar un abuso en el ejercicio del mando, lo que nos llevaría a una vulneración de bienes jurídicos de naturaleza militar en unos tipos penales pluriofensivos en los que se protegen no solo derechos personalísimos de la persona como son su intimidad personal, su propia imagen, el honor, sino también la disciplina[20].

Estas modalidades de abuso podrían, en función de su contenido o reiteración, llegar a revestir las características del trato degradante al que se refiere el artículo 47 CPM[21].

---

[20] El Derecho Militar no regula ningún tipo penal, específico, cuya finalidad sea proteger la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, sin embargo, si se analizan las figuras delictivas expuestas, vemos que el sujeto activo de las mismas puede ser un *«hacker»* o particular con conocimientos informáticos y medios técnicos, pero también es fácilmente imaginable que miembros de las Fuerzas Armadas y de la Guardia Civil que disponen de esos conocimientos y medios técnicos puedan realizar esas conductas por extralimitación de sus funciones o por una utilización ilegítima de los medios a su cargo.

[21] Así, la jurisprudencia del Tribunal Europeo de Derechos Humanos, al interpretar el art. 3.º del Convenio de Roma (SSTEDH de 18.01.78; 25.04.78; 25.02.82; 28.05.85; 27.08.92; 09.12.94; 28.11.96 y 10.05.01) resoluciones todas ellas en las que el TEDH perfila el concepto de «trato degradante» en los supuestos de afectación de la dignidad, en la existencia de humillación ocasionada por la conducta que los origina y en los efectos psicológicos desfavorables para la víctima; describiendo que los malos tratos «han de revestir un mínimo de gravedad», significando que «la apreciación de ese mínimo es cuestión relativa por su propia naturaleza, que depende del conjunto de los datos del caso, y especialmente de la duración de los malos tratos y de sus efectos físicos o mentales y, a veces, del sexo, de la edad, del estado de salud de la víctima, etc., debiendo analizarse también el hecho de que los tratos degradantes creen en las víctimas sentimientos de temor, de angustia y de inferioridad, susceptibles de humillarles, de envilecerles y de quebrantar en su caso su resis-

Conforme a la reiterada Jurisprudencia, establecida por la Sala Quinta, para estimar que existe *«trato degradante»*, en el ámbito militar, debemos hallarnos ante cualquier atentado a la dignidad de la persona que lesione su integridad moral de forma grave de manera que, objetivamente, pueda generar sentimientos de humillación y vejación, debiendo tenerse, especialmente, en cuenta el contenido de las Reales Ordenanzas para las Fuerzas Armadas aprobadas por Real Decreto 96/2009, de 6 de febrero, que establece en su artículo 11, lo siguiente, acerca del militar:

> *«Ajustará su conducta al respeto de las personas, al bien común y al derecho internacional aplicable en conflictos armados. La dignidad y los derechos inviolables de la persona son valores que tienen obligación de respetar y derecho a exigir. En ningún caso los militares estarán sometidos, ni someterán a otros, a medidas que supongan menoscabo de la dignidad personal o limitación indebida de sus derechos»*.

Cuando se trate de militares de igual empleo, se podrá acudir a lo dispuesto en los artículos 49 y 50, en los que no se exige que exista relación jerárquica.

En el caso de que esa intromisión ilegítima sea realizada por el subordinado, no parece oportuno acudir a los tipos de insulto a superior en los que se recogen como conductas típicas *coaccionar, amenazar, injuriar en su presencia por escrito o con publicidad al superior, poner mano en arma ofensiva, ejecutar actos o demostraciones con tendencia a maltratar de obra al superior o realizar de forma efectiva ese maltrato,* conductas que, analizadas, literalmente, hacen complicado incluir en ellas la acción del subordinado que realiza una intromisión ilegítima en la intimidad del superior. Lo más plausible, a nuestro juicio, sería hacer uso de los artículos 49 y 50 CPM.

6.1.4. *Delitos contra la eficacia del servicio*

Recogidos en los siguientes:

---

tencia física o moral». Esta jurisprudencia europea ha sido luego ratificada por el Tribunal Constitucional (SS de 29.01.08; 11.04.08 y 27.06.90 y por esta Sala de lo Militar en numerosas Sentencias 30.10.90; 14.09.92; 23.03.93; 12.04.94; 29.04.97; 25.11.98 y 20.12.99, entre otras), haciendo siempre hincapié en que la humillación o degradación del superior y el desprecio al valor fundamental de la dignidad humana han de ser valorados para la configuración del tipo delictivo del artículo 106 CPM en su modalidad de trato degradante.

Artículo 73 CPM

El militar *que,* ***en situación de conflicto armado o estado de sitio y por imprudencia grave****, causare los daños previstos en los artículos 264 a 266 del Código Penal, ocasionare que los medios o recursos de la Defensa o Seguridad nacionales caigan en poder del enemigo, perjudicare gravemente una operación militar, será castigado con la pena de seis meses a cuatro años de prisión.* ***Fuera de la situación de conflicto armado o estado de sitio*** *se impondrá la pena de prisión de tres meses y un día a dos años.*

Nos remitimos a propósito de este artículo a lo ya expuesto acerca del artículo 27 CPM, por remitirse a los mismos preceptos del Código Penal.

Artículo 75 CPM

Será castigado con la pena de tres meses y un día a dos años de prisión el militar que:

1.º ***Ejecutare o no impidiere*** *en lugar o establecimiento afecto a las Fuerzas Armadas o a la Guardia Civil* ***actos que puedan producir incendio o estragos, u originare un grave riesgo para la seguridad de la fuerza, unidad, establecimiento, buque de guerra, buque de la Guardia Civil o aeronave militar****…*

3.º ***Incumpliere****, con infracción de lo establecido 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, sus* ***deberes militares fundamentales, o los deberes técnicos esenciales de su función específica, ocasionando grave daño para el servicio****, sin perjuicio de la pena que corresponda por los resultados lesivos producidos conforme al Código Penal. Cuando los hechos descritos en este apartado se cometieren por* ***imprudencia grave****, se impondrá la pena de tres meses y un día a seis meses de prisión o multa de dos a seis meses.*

Los autores de los tipos descritos pueden, perfectamente, servirse para su ejecución de las ventajas que ofrecen las TIC, pudiendo en tales casos, además, entrañar una especial complejidad su investigación y exigir conocimientos específicos en la materia, entrando, por tanto, dentro del concepto de delitos informáticos que hemos adoptado.

6.2. Otros tipos penales incluibles

Junto a los antes señalados hay otros tipos que, asimismo, se encontrarían dentro de la clasificación que hemos adoptado, aunque nos limitaremos a mencionarlos, dada su escasa presencia estadística. Señalar, como principal argumento para su inclusión el hecho de que para su investigación, según la forma comisiva utilizada, pudieran requerirse especiales conocimientos sobre las TIC. Entre ellos podemos mencionar los siguientes:

> *«**Artículo 24. Traición militar*** En los supuestos de *3.º* ***Propalare o difundiere noticias desmoralizadoras o realizare cualesquiera otros actos derrotistas**. 4.º* ***Ejecutare actos de sabotaje**, dificultare las operaciones bélicas o de cualquier otro modo efectivo causare quebranto a los medios o recursos afectos a la defensa militar.*
>
> ***Artículo 25**. **Espionaje militar.** El extranjero que, en situación de conflicto armado, **se procurare, difundiera, falseare o inutilizare información clasificada como reservada o secreta o de interés militar susceptible de perjudicar a la seguridad o a la defensa nacionales, o de los medios técnicos o sistemas empleados por las Fuerzas Armadas o la Guardia Civil o las industrias de interés militar, o la revelase a potencia extranjera, asociación u organismo internacional**,…*
>
> ***Artículo 28**. El militar que **denunciare falsamente la existencia, en lugares afectos a las Fuerzas Armadas o a la Guardia Civil, de aparatos explosivos u otros similares o entorpeciere intencionadamente el transporte, aprovisionamiento, transmisiones** o cualquier clase de misión militar…*
>
> ***Artículo 29**. 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**….*
>
> ***Artículo 30**. **Incumplimiento de bandos militares en situación de conflicto armado o estado de sitio».***

Habrá de estarse al contenido de los bandos para determinar si, la comisión de los delitos incluidos en ellos, es susceptible de hacerse mediante la utilización de las TIC.

Artículo 51. Cobardía. *1. El militar que* ***por temor a un riesgo personal*** *(…) realizare* ***actos susceptibles de infundir pánico o producir grave desorden*** *entre la propia fuerza…*

Artículo 55. Deslealtad. *El militar que sobre asuntos del servicio diere a sabiendas* ***información falsa o expidiere certificado en sentido distinto al que le constare****…* Mediante utilización de las TIC.

Artículo 79. Delitos contra otros deberes del servicio. *El militar que usare pública e intencionadamente uniforme, divisas, distintivos o insignias militares, medallas o condecoraciones que no tenga derecho a usar ,...*

Realizando la conducta descrita, en actividades de carácter público y abierto, ya sea en: portales; foros; webs; Blogs; Facebook; u otros medios de similar difusión general y pública en la red.

Artículo 81. Delitos contra el patrimonio en el ámbito militar

1. El militar que, simulando necesidades para el servicio o derechos económicos a favor del personal, ***solicitare la asignación de crédito presupuestario para atención supuesta*** *...*

Artículo 82

1. El militar que cometiere los delitos de ***hurto, robo, apropiación indebida o daños previstos en el Código Penal en relación con el equipo reglamentario, materiales o efectos que tenga bajo su custodia o responsabilidad por razón de su cargo o destino*** *...*

Artículo 83

El militar que, prevaliéndose de su condición, se procurase intereses en cualquier clase de contrato u operación que afecte a la Administración militar o cometiese el delito previsto en el artículo 441 del Código Penal*…*

Artículo 84

El particular o empresario *que, en situación de conflicto armado o estado de sitio, habiendo contratado con la Administración Militar,* ***incumpliere en su integridad las obligaciones contraídas o las cumpliere en condiciones defectuosas que desvirtúen o impidan la***

finalidad del contrato, cuando resulten afectados los intereses de la Defensa nacional*...*

Artículo 85

El que, ***con ánimo de lucro y con conocimiento de la comisión de un delito contra el patrimonio*** *en el ámbito militar en el que no haya intervenido ni como autor ni como cómplice,* ***ayude a los responsables a aprovecharse de los efectos del mismo o reciba, adquiera u oculte tales efectos****...*

La utilización de las TIC, está hoy presente en todas la actividades económicas: pasaportes; dietas; asignación de créditos; pagaduría; contratación; contabilidad; etc., que se realizan en el ámbito de la defensa, como también sucede en la vida civil, ya sea por la presentación o libramientos de documentos en soporte electrónico, intercambio de correos electrónicos sobre los mismos o sobre contratos u operaciones que se realizan, o también por el archivo temporal o final de toda la documentación económica tramitada en soportes digitales, siendo por ello imprescindible para su adecuada investigación especiales conocimientos sobre TIC.

7. LAS FALTAS DISCIPLINARIAS

La Ley Orgánica 8/2014, de Régimen Disciplinario de las Fuerzas Armadas de 4 de diciembre de 2014, si bien solo en un caso, menciona la posible comisión telemática (*Artículo 6. número 4. Expresar públicamente opiniones que, relacionadas estrictamente con el servicio en las Fuerzas Armadas, no se ajusten a los límites derivados de la disciplina, realizadas cualesquiera de ellas de palabra, por escrito o por* ***medios telemáticos***), incorpora una gran cantidad de faltas disciplinarias susceptibles de cometerse mediante las TIC.

No obstante, lo dicho hasta el momento, a propósito de los delitos, difícilmente sería aplicable a las faltas disciplinarias, pues, en ellas, no existe la posibilidad de solicitar la cesión de los datos identificativos, por parte de las operadoras, al subordinarse esta conforme al art. 1.1 de la ley a «*la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales».* La limitación de la autorización al caso de los delitos graves conforme al criterio del artículo 33 CP podría dejar impunes múltiples delitos, ya no digamos faltas disciplinarias, cometidos por Internet o

telefonía, supondría cortar de raíz la posibilidad de investigar conductas que utilizando tecnologías de la información y la comunicación y teniendo gran trascendencia social, no alcanzan por la penalidad asignada el rango de delito grave[22]. En definitiva, con el marco jurídico vigente, toda investigación policial o del Ministerio Fiscal para el esclarecimiento de un hecho ilícito que requiera la cesión de alguno de los datos almacenados por las operadoras impondrá de forma incuestionable autorización del Juez de Instrucción.

Hemos de señalar, no obstante, que en la Ley Orgánica 12/2007, de 22 de octubre, del Régimen Disciplinario para la Guardia Civil, se incluyen supuestos específicos de ilícitos informáticos disciplinarios estos son como:

- **Faltas graves artículo 8**, números:

16. *Instalar u ordenar la instalación de videocámaras fijas o medios técnicos análogos para fines previstos por la Ley, sin cumplir todos los requisitos legales.*

17. *Incumplir las condiciones o limitaciones fijadas en la resolución por la que se autorizó la obtención de imágenes y sonidos por el medio técnico autorizado.*

18. *Utilizar u ordenar la utilización de videocámaras móviles, sin cumplir todos los requisitos exigidos por la Ley.*

19. *Conservar las grabaciones lícitamente efectuadas con videocámaras o medios técnicos análogos por más tiempo o fuera de los casos permitidos por la Ley, o cederlas o copiarlas cuando la Ley lo prohíbe.*

20. *Cualquier otra infracción a la normativa legal sobre utilización de medios técnicos de captación de imágenes y sonidos por las Fuerzas y Cuerpos de Seguridad en lugares públicos.*

- **Faltas muy graves artículo 7,** números:

20. *Permitir el acceso de personas no autorizadas a las imágenes o sonidos obtenidos por cualquier medio legítimo o utilizar aquéllas o éstos para fines distintos de los previstos legalmente.*

[22] La jurisprudencia del TS ha establecido que una medida de investigación judicial que afecta tan directa y gravemente a la intimidad de las personas solo puede encontrar su justificación, en el ámbito del proceso penal, cuando lo que se persiga sea un delito grave, en el bien entendido de que no solo ha de tenerse en cuenta la gravedad de la pena, sino también su trascendencia y repercusión social (SSTS n.º 740/2012, de 10 de octubre; 467/1998, de 3 de abril; 622/1998, de 11 de mayo).

21. *Reproducir las imágenes y sonidos obtenidos con videocámaras para fines distintos de los previstos legalmente.*
22. *Utilizar los medios técnicos regulados en la normativa legal sobre videocámaras para fines distintos de los previstos en ésta.*

Por ultimo llamar la atención sobre las conductas constitutivas de ilícito disciplinario, en que su calificación no es parangonable con la alarma que pueden producir, como: obtener y publicar fotografías de bajas propias u hostiles, conductas exhibicionistas o agresivas en recintos militares, hechas en principio para el autor o un grupo limitado de personas pero que al entrar por cualquier medio en la red alcanzan una repercusión desmesurada.

8. CONCLUSIONES

El vertiginoso ritmo de evolución, en el campo en que nos movemos, hace difícil adaptar la norma penal y procesal a la realidad cambiante a la que ha de ser aplicada, ello exigirá tipos penales que sin alejarse de la necesaria precisión en la tipificación de las conductas (principios de tipicidad y legalidad penal), ofrezcan posibilidad de adaptarse a la nuevas formas de comisión delictiva, así como, normas procesales que avalen métodos de investigación más ágiles y eficaces, en la línea de los introducidos por la L. O. 13/2015, que, con salvaguarda de los derechos en juego, permitan la adecuada persecución de los delitos cibernéticos, los existentes y los que vayan surgiendo, evitando cualquier situación de impunidad.

La especialización. Entendiendo como tal, en una jurisdicción como la nuestra, ya de por sí especializada, no la adscripción más o menos exclusiva de personal a esta función, lo cual no parece necesario, sino el favorecimiento de una mayor formación del mismo en la materia, para que cuando nos encontremos ante un delito cometido mediante las TIC, que debamos investigar, sepamos cómo hacerlo, qué instrumento técnicos tenemos y hasta dónde se puede llegar en la investigación con los medios existentes.

Parece más adecuado, adoptar un punto de vista amplio a la hora de enfocar el delito informático, pues, en definitiva, tal y como hemos intentado explicar se trata de delitos, en su mayoría muy conocidos, pero cuya especialidad está a la hora de probar la vinculación del autor al hecho, la prueba que recae sobre las TIC presenta un plus de dificultad, ya sea por la aludida dificultad de identificar al autor como por la necesidad de actuar con criterios distintos a la hora de determinar y reflejar en los autos, as-

pectos de la conducta típica como su gravedad, los daños producidos o la publicidad alcanzada.

La protección jurídico penal de los medios asignados a las Fuerzas Armadas, iniciada por el CPM, debe incrementarse en razón de la progresiva importancia de las TIC, para su normal funcionamiento, pues constituyen el nervio esencial de su operatividad, y, ello pone de relevancia la necesidad de una máxima protección frente a ataques tanto exteriores, como los efectuados desde el interior aun cuando estos puedan tener origen en conductas culposas o negligentes.

Por último, y dada la constatación de la cantidad de ilícitos disciplinarios, de importante trascendencia, que se cometen mediante el uso no autorizado de *smartphones*. Sería conveniente reflexionar sobre la necesidad o no, de que estos dispositivos acompañen al soldado en todo momento de su vida militar, haciendo posible, mediante la subida a la red de contenidos de muy diverso cariz, con escasa conciencia de su relevancia social y, en algunos casos, incluso, penal, una retrasmisión en vivo y en directo de los momentos más delicados de la vida de las unidades, sobre todo en situaciones de conflicto.

BIBLIOGRAFÍA

− CHICHARRO LÁZARO, ALICIA, *La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas*. IDP: revista de Internet, derecho y política, revista d'Internet, dret i política, n.º 9, 2009.

− DE LA MATA BARRANCO NORBERTO.J, HERNÁNDEZ DÍAZ LEYRE. «*El delito de daños informáticos: una tipificación defectuosa» Estudios penales y criminológicos,* n.º 29, 2009, pp. 311-362.

− DÍAZ GÓMEZ, ANDRÉS, «*El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest»*. Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR 8, diciembre 2010, pp. 169-203.

− HERNÁNDEZ DÍAZ, LEYRE. *«El Delito Informático*», Cuaderno del Instituto Vasco de Criminología, n.º 23, 2009, pp. 227-243.

− ROVIRA DEL CANTO, ENRIQUE. *Las nuevas pruebas telemática y digitales. Especialidad de la prueba en delitos cometidos por internet.* Conferencia presentada en el Consejo General del Poder Judicial. Jornadas sobre la prueba en el Proceso Penal. Estudios Jurídicos, Ministerio Fiscal, vol. I-2003. C. E. J. A. J. Madrid, 2003.

− ROVIRA DEL CANTO, ENRIQUE. *Delincuencia Informática y fraudes informáticos*, Editorial Comares, Granada, 2002.

− VELASCO NÚÑEZ, ELOY. *Delitos cometidos a través de Internet. Cuestiones Procesales.* La Ley- Actualidad, 2010.