ILÍCITOS MILITARES COMETIDOS A TRAVES DE INTERNET O CON OCASIÓN DEL USO DE LAS NUEVAS TECNOLOGÍAS (I).
DELIMITACIÓN Y PROBLEMAS PROCESALES Y DE PRUEBA QUE PLANTEAN.

Marcelo Ortega Gutiérrez-Maturana

Coronel Auditor

Fiscal Jefe del Tribunal Militar Territorial Tercero

RESUMEN

Se examina en este trabajo la trascendencia que tiene el uso de las TICs (Tecnologías de la información y comunicación) en la comisión de los ilícitos cometidos por militares, competencia de la jurisdicción militar, como amén de incorporar nuevas formas delictivas con especialidades en su comisión que tienen directa repercusión en la descripción típica y en la forma en que ha desarrollar la labor investigadora, afectan a la forma en que ha de realizarse la labor instructora, con la incorporación al procedimiento de un elenco de pruebas diferentes de las habituales, tanto en cuanto al fondo como a la forma de obtenerlas, que exigen la adopción de especiales precauciones para evitar que se frustre la labor investigadora así como la vulneración innecesaria de derechos fundamentales. Para situar adecuadamente el objeto de nuestro estudio haremos referencia, en primer lugar al marco en que nos movemos, así examinaremos brevemente: El denominado Derecho Informático, describiremos, si quiera, 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. Mas 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.

SUMARIO

1. **INTRODUCCION.**

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, si quiera, 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. Mas 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: 1º el régimen jurídico del software; 2º el derecho aplicable a las Redes de transmisión de datos; 3º los documentos electrónicos; 4º los contratos electrónicos; 5º el régimen jurídico de las bases de datos; 6º el derecho de la denominada "*privacy";* 7º los delitos informáticos; y 8º con carácter residual, otras conductas nacidas del uso de los ordenadores y de las redes de transmisión de datos[1].

Existían distintas opciones posibles, una, abordar la regulación o estudio de los aspectos relativos al ámbito de digitalización del mundo empresarial, administrativo e incluso personal desde un punto de vista sectorial, atribuyéndoselo a cada una de las ramas del ordenamiento jurídico ya existentes, y encajando en ellas las nuevas realidades en función del aspecto concreto a analizar. Así, de los contratos electrónicos se ocuparía el Derecho civil o mercantil, de las conductas ilícitas vinculadas a las nuevas tecnologías el Derecho Penal, Procesal o Administrativo, etc. 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] Seguiremos en este apartado el desarrollo que propone Hernández Díaz, Leyre: "*El delito informático"*, Revista Eguzkilore, Número 23, San Sebastián, Diciembre 2009, pp. 227 – 243.

1.2. LAS TICS (TECNOLOGÍAS DE LA INFORMACION Y COMUNICACIÓN), HITOS EN SU EVOLUCIÓN Y APARICIÓN DE NUEVAS CONDUCTAS Y FORMAS DE COMISÍON 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 cambio y desarrollo constante, igualmente rápido, de las conductas delictivas vinculadas a estas.

Antes de intentar exponer un concepto de delito o delitos informático o informáticos 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 TICs, 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

---

[2] En tal sentido, Ferreyros Soto, Carlos, *"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.

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

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 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, éstas 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 no hayamos inmersos con la aparición de la última generación de telefonía móvil multifuncional y de aparatos asistentes personales digitales (PADs) 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 sólo por el intercambio de datos, en gran cantidad y con mayor celeridad, comprendiendo voz, texto, música, fotografías o incluso películas, sino incluso 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 sólo 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 a través de Internet a 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 sólo en los ámbitos civil, social y administrativo, sino también 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 la conducta criminal 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 sólo pueden ser cometidos por cualquiera, sino que también amenazan a cualquier ciudadano*, y ha desarrollado nuevos supuestos de comisión delictiva, como, por ejemplo los abusos telefónicos, la

---

[4] Rovira Del Canto, Enrique: "*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.

[5] Morón Lerma, Esther: *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, colección RdPP monografía, Ed. Aranzadi, Pamplona, 1999, pág. 79.

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 sólo 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 sólo 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*. E Internet y las redes telemáticas traen consigo un nuevo concepto superador del tradicional de delito informático, el de ciberdelito o delito cibernético[6].

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[7]: "*LIBERTAD SI, 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 (música, 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

---

[6] Es con el X Congreso de las Naciones Unidas sobre la Prevención del Delito y el Tratamiento del Delincuente, celebrado en Viena del 14 al 17 de abril de 2000 (A/CONF.187), donde el análisis de la delincuencia informática o cibercriminalidad vuelve a tener su espacio significativo propio, y se partió de un concepto del delito cibernético como "todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos", abarcando, en principio, "todo delito que puede cometerse en un medio electrónico", y utilizando la palabra "delitos" para designar "formas de comportamiento generalmente definidas como ilegales o que probablemente serán declaradas ilegales en breve plazo", siendo posible que determinada conducta estuviera tipificada como delito en un Estado y no en otros, pero sobre el sentido dado en un entendimiento común internacional en cuanto al tipo de comportamiento relacionado con los sistemas y redes informáticos que debe declararse ilegal. En tales términos establece dos subcategorías de delitos cibernéticos: a) Delito cibernético en sentido estricto ("delito informático"): todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y los datos procesados por ellos; b) Delito cibernético en sentido lato ("delito relacionado con ordenadores"): todo comportamiento ilícito realizado por medio de un sistema o una red informáticos, o en relación con ellos; incluidos los delitos como la posesión, el ofrecimiento o la distribución ilegales de información por medio de un sistema o una red informáticos. Rovira Del Canto, Enrique: *Hacia una expansión doctrinal y fáctica del fraude informático"*, Revista Aranzadi de Derecho y Nuevas Tecnologías, núm. 2003-3, Edit. Thomson-Aranzadi, Pamplona, 2003, págs 115 y 116.

[7] Rovira Del Canto, Enrique: "*Las nuevas pruebas...*", op. cit. Pág. 283.

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 Ejercito Chino, intercepción masiva de comunicaciones realizada por la Agencia Nacional de Inteligencia americana[8] o espionaje generalizado de las delegaciones participantes en la Cumbre del G-20 celebrada en 2009 en el Reino Unido[9].

---

[8] 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. …** El caso del espionaje masivo de los EEUU ha puesto en la lista de prioridades de la Comisión la regulación en la materia, ya que como expresó la vicepresidenta de la Comisión Europea y responsable de Justicia, Viviane Reding, *"Este caso demuestra que un marco legal para la protección de datos personales no es un lujo, sino un derecho fundamental. Ya es hora de que el Consejo Europeo demuestre que puede actuar rápidamente para reforzar los derechos de los ciudadanos"*. La Comisión tiene muchos puntos que aclarar con EEUU, 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

[9] 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.** Al parecer los servicios de inteligencia interceptaron las llamadas telefónicas de móviles y los correos electrónicos de muchos de los asistentes a la mencionada cumbre. Nuevamente, la información publicada por "The Guardian" se basa en los documentos revelados por el ex trabajador de la Agencia de Seguridad Nacional de Estados Unidos, Mark Snowden, que asegura que el Cuartel General de Comunicaciones del Gobierno de Reino Unido (GCHQ), utilizó tecnología punta para interceptar las comunicaciones de los miembros de delegaciones extranjeras. Presuntamente, el espionaje no sólo consistió en la intervención de las comunicaciones vía móvil, si no que se pusieron en marcha cibercafés programados para controlar los correos electrónicos y claves de los delegados, información que llegaba a 45 analistas de inteligencia desplegados especialmente para ello, que la hacían llegar a su vez a los negociadores británicos en tiempo real. El objetivo del espionaje de las comunicaciones de participantes en la cumbre era conocer, de manera anticipada, cuáles era la verdadera postura de cada una de las delegaciones al respecto de las negociaciones, con lo que la británica contaba con ventaja sustancial para negociar de acuerdo a sus intereses. Hasta el momento, las autoridades británicas no han querido confirmar ni desmentir toda esta información, aunque sí han asegurado que sus servicios de inteligencia han actuado siempre conforme a la ley. La Comisión de Inteligencia y Seguridad de los Comunes será la responsable de realizar la investigación sobre la supuesta trama de espionaje. La publicación de esta nueva "entrega" de los documentos de Snowden coincide con la celebración de la cumbre de jefes de Estado o de

Pero libertad, se reitera, no puede significar impunidad. Y ello incluso viene reconocido no sólo 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[10] 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 aún 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 este último ámbito el 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[11], 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, alterando 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.

Gobierno del G-8 que se celebra este lunes y el martes en Irlanda del Norte, de nuevo, bajo la presidencia británica (que la ostentaba en el 2009).

[10] 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 mas segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos"* -eEurope 2002- (CES 115/2001).

[11] Velasco Nuñez, Eloy: "D*elitos cometidos a través de Internet. Cuestiones Procesales".* La Ley- Actualidad, 2010.

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[12] de los delitos informáticos que se expondrá a continuación:

3.1.1 **Ciberdelincuencia económica:** Delitos económico patrimoniales vinculados a la informática.

Se trata de los ataques al bien jurídico patrimonio ajeno, 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 o el descubrimiento y revelación de secretos relativos a la defensa nacional.

[12] Sieber, Ulrich: *Computerkriminalitat und Strafrecht,* Koln-Berlin-Bonn-München, Carl Heymanns Verlag KG, 1980, págs. 22 y ss

3.2. INSTRUCCIÓN 2/2011 DE LA FISCALIA GENERAL DEL ESTADO. Junto a la clasificación expuesta expondremos por su interés, en nuestro caso, 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, figura de la que mas adelante tendremos ocasión de ocuparnos. Esta, meramente instrumental, cuya adopción explica la propia Instrucción[13] es la que sigue, relacionándola con su calificación jurídica penal en el actual Código Penal, tras la modificación operada por la Ley Orgánica 5/2010 de 22 de Junio, que tipifica específicamente determinadas 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 TICs.**

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

---

[13] "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.

No obstante, esta circunstancia no debe llevarnos sin más a considerar que cualquier conducta delictiva en cuya ejecución se haga uso de las tecnologías de la información y la comunicación ha de incluirse en la categoría que nos ocupa, pues ello daría lugar a una desnaturalización del concepto, tal y como viene siendo considerado internacionalmente, e incluso a un desbordamiento del propio planteamiento de la especialización en este ámbito. Exigencias mínimas de operatividad y eficacia demandan, por tanto, una mayor concreción en la delimitación del objeto de actividad en este área de trabajo de tal forma que únicamente alcance su competencia, 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.

Por otra parte, es un hecho cierto que los inconvenientes apuntados en orden a definir el marco objetivo de actividad de esta especialidad, se hacen más evidentes si se tiene en cuenta que el ritmo de evolución de la ciencia y la tecnología hacen aconsejable, en el momento presente, no limitar, en un catálogo cerrado, los tipos penales susceptibles de encuadrarse en la categoría de criminalidad informática, ya que es más que previsible la aparición, en un futuro más o menos próximo, de nuevas formas de delincuencia o nuevos mecanismos de comisión de ilícitos ya tipificados, en los que el elemento determinante sea también la utilización de las tecnologías de la información y la comunicación (en adelante TICs), de forma tal que su análisis y valoración demande de conocimientos específicos que hagan aconsejable su asignación a quienes integren este área de actividad del Ministerio Fiscal.

Todas estas circunstancias determinan que el catálogo inicial de delitos a los que se extiende el marco competencial del área de criminalidad informática, que a continuación se expone estructurado en tres categorías, 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 acceso sin autorización a datos, programas o sistemas informáticos previstos y penados en el artículo 197.3 del Código Penal.

-Delitos de descubrimiento y revelación de secretos del artículo 197 del Código Penal cometidos a través de las TICs 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 TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos ó 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 TICs.**

-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 TICs para llevar a efecto la transferencia u operación de cualquier tipo en perjuicio de otro.

-Delitos de acoso a menores de 13 años, *child grooming*, previstos y penados en el art. 183 bis del Código Penal cuando se lleve a efecto a través de las TICs.

-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 TICs.

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

3.2.3. **Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, 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 TICs 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 211 y ss del Código Penal cometidos a través de las TICs 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 TICs 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 TICs 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 607.2 del Código Penal cometidos a través de las TICs 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 TICs 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 termino su investigación. En el ámbito del derecho procesal y de la obtención de pruebas de la comisión de delitos, no sólo los delitos informáticos *strictu 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.

Ya el Consejo de Europa, en sus Recomendaciones de 1989 y 1995, (R (89) 9 y R (95) 13); subrayó la necesidad de que las autoridades nacionales, policiales o gubernativas, encargadas de aplicar la ley establecieran departamentos u oficinas especializadas en delitos informáticos, dotadas de personal adecuado y de equipos programas informáticos apropiados, personal capacitado y con conocimientos técnicos al día, y programas de especialización. Muchos Estados, entre ellos el nuestro, como luego tendremos ocasión de examinar, han creado departamentos policiales especializados en delincuencia informática -tanto el Cuerpo de Policía Nacional, como la Guardia Civil, entre otros, cuentan con

ellos[14]- fiscales especializados en delitos informáticos, como veremos a continuación, e 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 éstas 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 realzado 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 sólo el carácter intangible de los datos y de la información que contienen, sino el carácter 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 ejemplo, el autor *"lanza"* a través de la red un virus tipo *"bomba lógica"* pero inactivo, que se va introduciendo en determinados y seleccionados sistemas o equipos, o incluso aleatoriamente, pero no se activa hasta una fecha determinada o recibir una instrucción encriptada por vía telemática en tal sentido. Por otro lado, la característica del distanciamiento espacial, esto es, el que el sujeto se encuentre físicamente distante no sólo del lugar donde se materializan los efectos de su comportamiento ilícito, sino incluso de aquél 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.

[14] 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.

4.1 LA ESPECIALIZACIÓN FISCAL EN MATERIA DE CRIMINALIDAD INFORMÁTICA.

En nuestro marco de actuación, Ministerio Fiscal, se han dado pasos muy importantes en este sentido, un hito, especialmente, importante lo constituye 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, por la que se crea esta figura.

4.1.1. **Fundamento.** Como explica la propia Instrucción el área de especialización en criminalidad informática surge como una necesidad constatada en la práctica habitual de las Fiscalías al haberse detectado un progresivo aumento en el número de investigaciones criminales vinculadas a la utilización de las nuevas tecnologías y más específicamente de internet, como red de redes. Es un hecho cierto que la generalización de estos instrumentos en el desarrollo de las relaciones económicas y sociales ha ido determinando la aparición de nuevas formas de criminalidad y posibilitando también dinámicas y mecanismos, hasta ahora no conocidos, en la comisión de conductas ilícitas de carácter más tradicional.

4.1.2 **Desarrollo.** La especialización se materializa mediante la creación de la figura del *Fiscal de Sala Coordinador para la Criminalidad Informática*, al que se asignan las siguientes funciones:

"1.- Practicar las diligencias a que se refiere el artículo cinco del Estatuto Orgánico del Ministerio Fiscal[15] *e intervenir directamente, o a través de instrucciones,*

[15] Artículo 5. Estatuto Orgánico del Ministerio Fiscal, aprobado por Ley 24/2007 de 9 de octubre:

"1. El fiscal podrá recibir denuncias, enviándolas a la autoridad judicial o decretando su archivo, cuando no encuentre fundamentos para ejercitar acción alguna, notificando en este último caso la decisión al denunciante.

2. Igualmente, y para el esclarecimiento de los hechos denunciados o que aparezcan en los atestados de los que conozca, puede llevar a cabo u ordenar aquellas diligencias para las que esté legitimado según la Ley de Enjuiciamiento Criminal, las cuales no podrán suponer la adopción de medidas cautelares o limitativas de derechos. No obstante, podrá ordenar el fiscal la detención preventiva.

Todas las diligencias que el Ministerio Fiscal practique o que se lleven a cabo bajo su dirección gozarán de presunción de autenticidad.

Los principios de contradicción, proporcionalidad y defensa inspirarán la práctica de esas diligencias.

A tal fin, el Fiscal recibirá declaración al sospechoso, quien habrá de estar asistido de letrado y podrá tomar conocimiento del contenido de las diligencias practicadas. La duración de esas diligencias habrá de ser proporcionada a la naturaleza del hecho investigado, sin que pueda exceder de seis meses, salvo prórroga acordada mediante decreto motivado del Fiscal General del Estado.

No obstante, las diligencias de investigación en relación con los delitos a que se hace referencia en el apartado Cuatro del artículo Diecinueve del presente Estatuto, tendrán una duración máxima de doce meses salvo prórroga acordada mediante Decreto motivado del Fiscal General del Estado.

3. Transcurrido el oportuno plazo, si la investigación hubiera evidenciado hechos de significación penal y sea cual fuese el estado de las diligencias, el Fiscal procederá a su judicialización, formulando al efecto la oportuna denuncia o querella, a menos que resultara procedente su archivo.

También podrá el fiscal incoar diligencias preprocesales encaminadas a facilitar el ejercicio de las demás funciones que el ordenamiento jurídico le atribuye."

Como detalla la propia Instrucción, arriba citada "*Esta asignación es factible tanto en relación*

en aquellos procesos penales de especial trascendencia apreciada por el Fiscal General del Estado, referentes a hechos delictivos relacionados con la Criminalidad Informática.

2.-Supervisar y coordinar la actividad de las secciones de Criminalidad Informática y recabar informes de las mismas, dando conocimiento al Fiscal Jefe del órgano del Ministerio Fiscal en que se integran.

3.- Coordinar los criterios de actuación de las distintas Fiscalías en materia de criminalidad informática, para lo cual podrá proponer al Fiscal General la emisión de las correspondientes Instrucciones y reunir cuando proceda a los Fiscales integrantes de las secciones especializadas.

4.- Elaborar anualmente y presentar al Fiscal General del Estado un informe sobre los procedimientos seguidos y actuaciones practicadas por el Ministerio Fiscal en materia de criminalidad informática que será incorporado a la Memoria anual presentada por el Fiscal General del Estado"[16].

---

con la apertura y tramitación de diligencias de investigación penal al amparo del artículo 5 del Estatuto Orgánico como en relación con procedimientos judiciales en curso".

[16] "*Además de estas funciones, expresamente previstas en la norma estatutaria, corresponden también al Fiscal de Sala de Criminalidad Informática las atribuciones que a continuación se detallan y que son inherentes al ejercicio de su función, en términos similares a los establecidos con carácter general para los Fiscales de Sala Delegados y Coordinadores de especialidades en la Instrucción 11/2005 y en las restantes Instrucciones de la Fiscalía General del Estado dictadas hasta el momento, en relación con las distintas especialidades.*

-Coordinar la intervención del Ministerio Fiscal en las investigaciones relativas a hechos comprendidos en el marco de actuación de la especialidad cuando afecten al territorio de más de una Fiscalía provincial y revistan especial complejidad o trascendencia. Con dicha finalidad mantendrá contacto permanente con los responsables de las unidades de policía judicial de ámbito nacional o autonómico dedicadas específicamente a esta materia, coordinando las instrucciones de carácter general que se impartan a las mismas en los términos previstos en la Instrucción 1/2008 de la Fiscalía General del Estado sobre dirección por el Ministerio Fiscal de las actuaciones de la Policía Judicial.

En el ejercicio de esta función el Fiscal de Sala Coordinador de Criminalidad Informática facilitará el contacto de los Fiscales especialistas con las unidades policiales del respectivo territorio y cuidará se mantengan debidamente informados los Fiscales Superiores y los Fiscales Jefes de los correspondientes órganos del Ministerio Fiscal.

-Mantener contacto con las autoridades administrativas con competencia en esta materia para resolver las cuestiones generales que, relacionadas con su función, puedan ir planteándose. Apoyar y facilitar, a su vez, la comunicación directa que los Fiscales especialistas deban establecer con las dichas autoridades en sus respectivos territorios.

-Promover la organización y celebración de actividades formativas, cursos, jornadas de especialistas o seminarios de especialización relacionados con la Criminalidad Informática y colaborar con la Secretaría Técnica en la determinación de criterios para la formación de Fiscales especialistas, dentro del marco de los planes de formación inicial y continuada de la Carrera Fiscal.

-Impulsar y participar en la adopción de Protocolos y Convenios de coordinación y colaboración con aquellos organismos e Instituciones implicados en la prevención, investigación y persecución de los comportamientos ilícitos relativos a esta materia". Instrucción 2/2011 de la Fiscalía General del Estado, antes citada.

El nombramiento del Fiscal de Sala Coordinador para la Criminalidad Informática, constituye el presupuesto de hecho para la creación de las respectivas secciones territoriales especializadas en los distintos órganos del Ministerio Fiscal, articulando de esta forma el despliegue territorial del área de especialización en Criminalidad Informática, en condiciones similares a las ya existentes en otras áreas, con lo que su ámbito territorial de actuación es provincial, debiendo constituirse, como mínimo, una por provincia que, generalmente, tendrá su sede en las Fiscalías Provinciales. Su dimensión y estructura interna es flexible para poder adaptarse a la plantilla, el volumen de actividad y las necesidades de cada uno de los órganos del Ministerio Fiscal. La adscripción de Fiscales de la plantilla, uno o más, a la sección se realizará, de acuerdo con lo que establece el propio Estatuto y no implica exclusividad. La dirección de estas secciones se encomienda a un Delegado Provincial. Tanto el Delegado de la especialidad como los Fiscales especialistas adscritos a la sección se encuentran bajo la dependencia jerárquica del Fiscal Jefe respectivo.

5. **PRINCIPAL NORMATIVA EN LA MATERÍA.**

Por razones obvias, nos limitaremos a indicar los textos fundamentales en la materia.

5.1. EL CONVENIO SOBRE CIBERDELINCUENCIA DEL CONSEJO DE EUROPA.

Los diversos gobiernos nacionales y organismos internacionales están trabajando en diversos ámbitos dirigidos a obtener tratados y convenios globales sobre los delitos informáticos. Como exponente mas 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 39 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 entro 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. Constituye 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 y sin perjuicio del examen mas detallado que se hará en la segunda parte de la Conferencia, 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 sólo 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 obtención, almacenamiento y creación de pruebas en el marco de investigaciones o procedimientos específicamente criminales.

5.2. LEGISLACION ESPAÑOLA

5.2.1. Las reformas mas importantes han sido la modificación del **Código Pena**l por Ley Orgánica 5/2010 de 22 de Junio, que tipifica específicamente determinadas conductas relacionadas con esta materia a las que ya hemos hecho referencia anteriormente y que sintetizaremos en las siguiente clasificación:

5.2.1.1. ***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
Art. 264.2 CP. Virus o daños informáticos, cuando se produce sobre datos. Cuando los daños persiguen a los sistemas informáticos (no a los datos en si mismo) estamos ante

un *sabotaje informático* que se castiga 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).

Art. 273 a 275 CP. Contra la propiedad industrial, con protección penal.

Art. 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. 301 CP. Blanqueo informático de capitales.

Art. 390 CP. Falsedad documental, cuando el soporte sea de naturaleza informática (art. 26 CP).

5.2.1.2. ***Ciberdelincuencia intrusiva.***

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

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

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

Art. 205 a 216 CP. Injurias y calumnias informáticas, con el art. 211 que califica de "delito" a las que se cometen a través de internet, excluyendo la falta por la difusión que alcanzan en ese medio.

Art. 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

5.2.1.3. ***Ciberterrorismo y ciberespionaje.***

Art. 402 CP. Usurpación de funciones públicas mediante correo electrónico
Art. 598 y 603 CP. Descubrimiento y revelación de secretos relativos a la defensa nacional

5.2.2. La Ley 25/2007, de 18 de octubre, de "***conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones"***, regula esta materia dictada en transposición de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. La Ley será detenidamente examinada en la segunda parte de la conferencia, si bien podemos adelantar que 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 ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

6. ESPECIAL REFERENCIA A LOS ILICITOS MILITARES.

6.1. EL CÓDIGO PENAL MILITAR.

El Código Penal Militar L.O.13/1985,de 9 de diciembre (en adelante CPM) no recoge ningún tipo en el que se penalicen conductas delictuales, típicamente, informáticas. Por ello no resulta de especial utilidad la clasificación tripartita (Ciberdelincuencia económica, intrusiva, Ciberespionaje y Ciberterrorismo) a que nos referimos al hablar de las clases de delitos informáticos, pues ninguna de estas figuras aparecen específicamente tipificadas en el CPM, ni los bienes jurídicos que, en ellos se protegen, son los mismos ha que hace referencia la legislación penal militar.

Ello evidencia como un texto, relativamente, moderno como el CPM se ha quedado obsoleto en cuanto al tratamiento de esta materia debido a su vertiginoso avance.

Sin embargo, el que no haya mención expresa en la normativa militar en relación a los comúnmente denominados delitos informáticos, no quiere decir que estos no puedan darse en la práctica. Por ello, desde un punto de vista práctico, adoptaremos el criterio recogido en la Instrucción de la Fiscalía General del Estado, 2/2011, que antes hemos tenido ocasión de examinar, al establecer su marco competencial que incluye: *además de los delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs.; aquellos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs.; y aquellos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia; así como finalmente cualquier otro tipo delictivo en cuya ejecución haya sido determinante la utilización de las TICs y en los que dicha circunstancia genere una especial complejidad en la investigación criminal*. Intentaremos incardinar las conductas descritas anteriormente en los tipos regulados en el CPM, en lo que sea posible.

6.1.1 **Tipos penales aplicados con mayor frecuencia.** Del examen de la documentación remitida por las diferentes Fiscalias, de las que se ha solicitado información y sin pretender un examen exhaustivo de la cuestión, resulta que el núcleo fundamental de delitos cometidos a traves de TICs en el ambito de la Jurisdiccion Militar se centra en los siguientes preceptos:

6.1.1.1. ***ESPIONAJE Y REVELACIÓN DE SECRETOS O INFORMACIONES RELATIVAS A LA SEGURIDAD NACIONAL Y DEFENSA NACIONAL.***

Estas conductas se integran con algunos preceptos del Código Penal Militar así el artículo 50 castiga como Espía la español que en tiempo de guerra realizase actos de espionaje militar, siendo castigado como traidor. También será punible tal conducta cuando la realice un militar en tiempo de paz. Consiste la conducta típica en procurarse, difundir, falsear o inutilizar información clasificada o de interés militar susceptible de perjudicar a la Seguridad Nacional o a la defensa nacional o de los medios técnicos o sistemas empleados por las Fuerzas Armadas o las industrias de interés militar.

En el artículo 53 CPM se castiga penalmente al militar que realizase esas conductas anteriormente descritas pero sin el propósito de favorecer a una potencia extranjera,

asociación u organismo internacional. La pena es inferior si la información no está legalmente clasificada. Los civiles igualmente pueden cometer esta conducta pero en tiempo de guerra.

El artículo 54 CPM recoge unos supuestos agravados para el caso de que el sujeto activo sea depositario o conocedor del secreto o información por razón de su cargo o destino o que la revelación consista en dar publicidad al secreto o información en algún medio de comunicación social o de forma que asegure su difusión.

En el artículo 55 CPM se castiga al militar que tenga en su poder, fuera de las condiciones fijadas en la legislación vigente, objeto, documento o información clasificada relativa a la Defensa Nacional; el mismo precepto castiga al militar que reproduzca planos o documentación referente a zonas, instalaciones o material militar de acceso restringido o reservado por su relación con la seguridad o la Defensa Nacional. Del mismo modo puede cometer el paisano estos delitos en tiempo de guerra.

Finalmente en el Código Penal Militar se recoge la posibilidad de cometer estas conductas imprudentemente, en el artículo 56, tanto por militares como por civiles en tiempo de guerra.

Los preceptos citados 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 ambito 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 juridico 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 los: clasificados y los no clasificados. Respecto de; 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. A su vez, 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 esta "clasificada" y no lleva sello, marca o distintivo alguno, puesto que sólo los clasificados lo llevan, 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 especifica. 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"*[17].

Incluiremos dentro de este apartado, por su similitud, pese a diferir en cuanto al bien jurídico protegido los:

DELITOS CONTRA LOS DEBERES DEL SERVICIO
CAPÍTULO II DESLEALTAD
Art. 115

El militar que sobre asuntos del servicio diere a sabiendas información falsa o expidiere certificado en sentido distinto al que le constare ...

Cuando en su información o certificado el militar, sin faltar sustancialmente a la verdad, la desnaturalizare, valiéndose de términos ambiguos, vagos o confusos, o la alterare mediante reticencias o inexactitudes, ...

Art. 116

El militar que no guardase la discreción y reserva debidas sobre asuntos del servicio de trascendencia grave .... Si la trascendencia no fuere grave ... por vía disciplinaria.

Estos preceptos, sobre todo el segundo, tienen una mayor amplitud, en cuanto su aplicación deriva de la mayor o menor gravedad del asunto sobre el que recae la conducta indiscreta han sido aplicados, si bien generalmente los supuestos se han remitido con posterioridad a la via disciplinaria.

---

[17] Auto de fecha 7 de septiembre de 2010, del Juzgado Togado Central nº1 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"*.

Esta exigencia aparece reforzada por la Ley Orgánica 9/2011, de 27 de julio, *"de derechos y deberes de los miembros de las Fuerzas Armadas",* 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."

6.1.1.2. ***DELITOS CONTRA LA DISCIPLINA***

CAPÍTULO I SEDICIÓN MILITAR

Art. 91

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, rehusaren obedecer las órdenes legítimas recibidas, incumplieren los demás deberes del servicio o amenazaren, ofendieren o ultrajaren a un superior …

Si le causare la muerte o lesiones al menos graves a un superior, se impondrá la pena de quince a veinticinco años de prisión a los promotores y demás responsables aludidos en el párrafo anterior, y de diez a veinticinco años a los meros ejecutores.

Art. 92

Se considerarán también reos de sedición militar los militares que, en número de cuatro o más, hicieren reclamaciones o peticiones colectivas en tumulto, con las armas en la mano o con publicidad.

Las demás reclamaciones o peticiones colectivas, así como las reuniones clandestinas para ocuparse de asuntos del servicio, …; sin embargo, podrán corregirse en vía disciplinaria si la trascendencia fuera mínima.

Art. 94

La conspiración y proposición para cometer el delito de sedición militar serán castigadas con la pena inferior a la respectivamente establecida para el tipo de delito de que se trate.

Las TICs posibilitan la realización de las conductas tipificadas, propiciando la ocultación de la identidad de los proponentes, o mediante la utilización del correo electrónico, en forma anónima o inidentificada o procedimientos similares[18]. Aunque el texto típico parece exigir la presencia corpórea, no es inimaginable que las reuniones clandestinas a que se refiere el artículo 93 CPM, pudieran realizarse "on line" o por, algún otro sistema de comunicación interactiva, como la videoconferencia.

CAPÍTULO II INSUBORDINACIÓN

Sección 1ª

INSULTO A SUPERIOR

Art. 101

El militar que, sin incurrir en los delitos previstos en los artículos anteriores, coaccionare, amenazare o injuriare en su presencia, por escrito o con publicidad, a un superior….

Es sin duda la mas frecuentes 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 ultima

[18] 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.

del autor de la comunicación, cuando se trata de una terminal particular compartida o un cibercafé.

También es concebible la inclusión, dentro de este concepto amplio de delito informático que venimos utilizando, de otros delitos de insulto a superior, en los que el conocimiento de los hechos o prueba de los mismos, provenga de grabaciones de video realizadas con smartphones o similares publicadas o subidas a la red por cualquier medio, pues la investigación de la certeza o no de los hechos grabados y de su autoría dependerían en gran medida de la investigación que se realizase sobre las evidencias digitales[19] dicha actividad de prueba, netamente incluida en la materia que estudiamos, constituiría el elemento clave para la determinación del hecho, así como la identificación de los autores.

CAPÍTULO III
ABUSO DE AUTORIDAD
Art. 103

El superior que, abusando de sus facultades de mando o de su posición en el servicio, irrogare un perjuicio grave al inferior, le obligare a prestaciones ajenas al interés del servicio o le impidiere arbitrariamente el ejercicio de algún derecho será castigado con la pena de tres meses y un día a cuatro años de prisión.

Art. 106

El superior que tratare a un inferior de manera degradante o inhumana ser castigado con la pena de tres meses y un día a cinco años de prisión.

Incluiremos junto a ellos por razones de oportunidad el artículo.

EXTRALIMITACIONES EN EL EJERCICIO DEL MANDO
Art. 138

El militar que en el ejercicio de su mando se excediere arbitrariamente de sus facultades o, prevaliéndose de su empleo o destino, cometiere cualquier otro abuso grave ….

Junto con contenido en el Artículo 101 CPM, constituye el núcleo fundamental de la delincuencia cometida mediante TICs 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 anteriormente, merman de forma importante la privacidad de los ciudadanos. Ello también ocurre, en el ámbito del Ministerio de Defensa y, si bien, el Derecho Penal Militar no castiga las posibles intromisiones que se pueden hacer a la intimidad de los militares, por vía de acceso ilegítimo a sus datos informáticos, sin embargo su necesaria protección resulta de la reciente 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

[19] v. gr., aunque se trate de un tipo delictivo distinto, sirve como ejemplo de forma de aparición de la "notitia criminis": el video presentado, recientemente, por el diario "El País" sobre presunto delito de maltrato a prisioneros por parte de tropas españolas durante la Guerra de Irak, que ha dado lugar a la incoación de las D.P. 12/015/13.

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 acciones 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, pudieran ser utilizados para castigar al superior que accediese de forma ilegítima a los datos informáticos privados de un subordinado, pues esta agresión a su intimidad, podría ser calificada, dependiendo de los supuestos, como una extralimitación en el ejercicio del mando, art 138 CPM, o como la conducta regulada en los artículos 103 ó 106 CPM, siempre y cuando por la relación entre superior y subordinado, la conexión con el servicio y la finalidad perseguida con la intromisión permitiesen observar 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 sólo derechos personalísimos de la persona como son su intimidad personal, su propia imagen, el honor, sino también la disciplina[20].

Las modalidades de abuso pueden llegar a revestir las características del trato degradante al que se refiere el artículo 106 CPM[21]

[20] El Derecho Militar no regula ningún tipo penal 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. 3º del Convenio de Roma (SSTEDH de 18.01.78 y 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 resistencia 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.

La definición de dicho trato en el ámbito militar tiene que incluir cualquier atentado a la dignidad de la persona que lesione su integridad moral de forma grave para 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. Dignidad de la persona:*

"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 tiene 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".

No se aplicara cuando no exista relación de jerárquica, sin perjuicio de la posible aplicación de los preceptos comunes.

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 el incluir en ellas la acción del subordinado que realiza una intromisión ilegítima en la intimidad del superior. Únicamente sería posible, y aún así de una forma bastante forzada, acudir a las coacciones[22].

6.1.2 **Otros tipos penales incluibles.** Junto a los antes señalados hay otros tipos que se encontrarian dentro de la descripcion hecha por la Fiscalia, que nos limitaremos a ennumerar, en cuanto su investigacion podría, según la forma comisiva, requerir especiales conocimientos sobre TICs, así:

ATENTADOS CONTRA LOS MEDIOS O RECURSOS DE LA DEFENSA NACIONAL

Art. 57

El que, en tiempo de guerra, intencionadamente destruyere, dañare o inutilizare para el servicio, aun de forma temporal, obras, establecimientos o instalaciones militares, buques, aeronaves, medios de transporte o transmisiones, vías de comunicación, material de guerra, aprovisionamiento u otros medios o recursos de la defensa nacional….

Art. 58

El militar que, en tiempo de paz, intencionadamente destruyere, dañare de modo grave o inutilizare para el servicio, aun de forma temporal, obras, establecimientos o instalaciones militares, buques de guerra, aeronaves militares, medios de transporte o transmisiones militares, material de guerra, aprovisionamiento u otros medios o recursos afectados al servicio de las Fuerzas Armadas …

Art. 59

El militar que denunciare falsamente la existencia, en lugar militar, de aparatos explosivos u otros similares o entorpeciere intencionadamente el transporte, aprovisionamiento, transmisiones o cualquier clase de misiones de los Ejércitos …

Art. 60

El militar que destruyere, inutilizare, falseare o abriere sin autorización la correspondencia oficial o documentación legalmente clasificada relacionada con la Seguridad Nacional o la Defensa Nacional.... En la misma pena incurrirá si tuviese en su poder sin autorización documentos clasificados.

[22] Blanco Álvarez, Fausto Manuel: *"Internet y la Infracción Penal"* Trabajo realizado para el Diploma de Derecho Penal Militar.

Art. 61

El que allanare una base, acuartelamiento o establecimiento militar, o vulnerase las medidas de seguridad establecidas para su protección ..

Art. 62

Cuando los delitos de este capítulo fueren cometidos por imprudencia serán castigados con la pena inferior en grado a la señalada en cada caso.

DELITOS CONTRA LA EFICACIA DEL SERVICIO

Art. 155

El militar que por imprudencia causare la pérdida, graves daños o inutilización para el servicio, aun de forma temporal, de plaza, fuerza, puesto, obras o instalaciones militares, medios de transporte o transmisiones, material de guerra, aprovisionamiento u otros medios y recursos de las Fuerzas Armadas, ocasionare que caigan en poder del enemigo o perjudicare gravemente una misión de guerra...

En tiempo de paz .. cuando se tratare de plaza, instalación militar, buque de guerra, aeronave militar o medio de transporte o transmisión o material de guerra.

Art. 157

Será castigado .. el militar que:

1. Ejecutare o no impidiere en lugar o establecimiento militar actos que puedan producir incendio o estragos, u originase un grave riesgo para la seguridad de una fuerza, unidad o establecimiento de las Fuerzas Armadas.

2. Ocultare a sus superiores averías o deterioros graves en instalaciones militares, buques de guerra o aeronave militar, medios de transporte o transmisiones, aprovisionamiento o material de guerra a su cargo.

4. Incumpliere sus deberes militares fundamentales, causando grave daño o riesgo para el servicio.

Art. 158

El militar que por negligencia no cumpliere una consigna general, dejare de observar una orden recibida o causare grave daño al servicio por incumplimiento de sus deberes militares fundamentales,... En tiempo de paz, si concurriere negligencia grave ....

Art. 159

El militar que se extralimite en la ejecución de un acto de servicio de armas reglamentariamente ordenado, ...; ...si causare lesiones muy graves, y ... si produjere cualquier otro tipo de lesiones o daños.

Si la muerte, lesiones o daños se produjeran por negligencia profesional o imprudencia .... En el caso de imprudencia temeraria y de que se tuviera la condición de militar profesional ...

Art. 160

Será castigado ... el militar que por impericia o negligencia profesional:

1. Dejare de transmitir a buque, aeronave u otra unidad militar las señales, marcaciones o mensaje a que está obligado, o los diere equivocados.

2. Encargado de proyectar o inspeccionar la construcción, reparación o modificación de buques de guerra, aeronaves militares, obras o material de las Fuerzas Armadas, consignare errores o reformas que perjudicaren su seguridad, eficacia o potencial bélico o consintiere obras o reformas no autorizadas.

3. Encargado del aprovisionamiento de las Fuerzas Armadas, dejare de suministrar municiones, repuestos, víveres, efectos o elementos de importancia para el servicio, los entregare adulterados o inservibles, o autorizare su recepción o uso a pesar de no reunir las condiciones necesarias.

4. Incumpliere los deberes técnicos de su profesión especial dentro de las Fuerzas Armadas.

Art. 161

Será castigado .. el militar que por negligencia:

1. Extraviare armas o material de guerra, procedimientos o documentación oficial que tuviera bajo su custodia por razón de su cargo o destino en las Fuerzas Armadas.

2. Diere lugar a la evasión de prisioneros de guerra, presos o detenidos, cuya conducción o custodia le estuviere encomendada.

CONTRA EL PATRIMONIO

DELITOS CONTRA LA HACIENDA EN EL ÁMBITO MILITAR

Art. 189

El militar que, simulando necesidades para el servicio o derechos económicos a favor del personal, solicitare la asignación de crédito presupuestario para atención supuesta …
Si las cantidades así obtenidas se aplicaren en beneficio propio…

Art. 190

El militar que empleare para sus fines particulares elementos asignados al servicio o los facilitare a un tercero, … a no ser que el hecho revista escasa entidad que será corregido por vía disciplinaria.

Art. 191

El militar que, prevaliéndose de su condición, se procurase intereses en cualquier clase de contrato u operación que afecte a la Administración Militar…

Art. 192

El militar que, encargado del aprovisionamiento de las Fuerzas Armadas, sustituyere unos efectos por otros o alterase sus cualidades fundamentales o características específicas…
En tiempo de guerra …

Art. 193

El que en tiempo de guerra 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 …. Los mismos hechos, cometidos por imprudencia, serán castigados con la pena de prisión de tres meses y un día a dos años.

Podrá imponerse, además, la suspensión de las actividades de la empresa por un período de uno a tres años y, en caso de especial gravedad, la incautación o disolución de la misma.

Art. 194

El militar que incumpliere las normas sobre material inútil, declarando como tal al que todavía se encontrase en condiciones de prestar servicio, o substrayendo al control reglamentario, en beneficio propio, al que merezca esta calificación ….

Art. 195

El militar que destruyere, deteriorare, abandonare o sustrajere, total o parcialmente, el equipo reglamentario, materiales o efectos que tenga bajo su custodia o responsabilidad por razón de su cargo o destino … siempre que su valor sea igual o superior a la cuantía mínima establecida en el Código Penal para el delito de hurto.

Art. 196

El militar que sustrajere o receptare material o efectos que, sin tenerlos bajo su cargo o custodia, estén afectados al servicio de las Fuerzas Armadas, …, siempre que su valor sea igual o superior a la cuantía establecida en el Código Penal para el delito de hurto.

Art. 197

El que, con conocimiento de su ilícita procedencia, adquiriere o tuviere en su poder los efectos a que hacen referencia los dos artículos anteriores,

En todos ellos es predicable la posible presencia de elementos de hecho o de prueba vinculados a las TICs, pues amén de que su comisión, en algunos de los tipos de ilícito militar expuestos, puede realizarse por medios informáticos o telemáticos, igualmente su conocimiento o la prueba de los mismos -como ya tuvimos ocasión de exponer al hablar de los delitos de insulto a Superior-, puede provenir de grabaciones de video realizadas con smartphones o similares publicadas o subidas a la red por cualquier medio, u otro tipo de evidencias digitales, para cuya investigación serian necesarios los conocimientos especializados al que nos hemos venido refiriendo.

6.2. ANTEPROYECTO DE CÓDIGO PENAL MILITAR 2013.

No podemos dejar de hacer mención a las reformas previstas en el Anteproyecto de ley de Código Penal Militar, que serán objeto de otra ponencia pero que, en la materia que nos ocupa, son especialmente significativos, así por remisión al Código Penal se incluirían:

6.2.1 **Daños.**

Artículo 75.

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…

Artículo 264

1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, o programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave...

2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave...

Artículo 265

El que destruyere, dañare de modo grave, o inutilizare para el servicio, aun de forma temporal, obras, establecimientos o instalaciones militares, buques de guerra, aeronaves militares, medios de transporte o transmisión militar, material de guerra, aprovisionamiento u otros medios o recursos afectados al servicio de las Fuerzas Armadas o de las Fuerzas y Cuerpos de Seguridad … si el daño causado excediere de cincuenta mil pesetas.

Artículo 266

1. Será castigado con pena de prisión de uno a tres años el que cometiere los daños previstos en el artículo 263 mediante incendio, o provocando explosiones o utilizando cualquier otro medio de similar potencia destructiva, poniendo en peligro la vida o la integridad de las personas…

6.2.2. **Revelación de secretos e informaciones relativas a la seguridad y defensa nacionales.**

Artículo 26.

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.

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.

CAPÍTULO III

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 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:

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

2º. 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. 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. … 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 destino ...

7. LAS FALTAS DISCIPLINARIAS.

En el Derecho Disciplinario Militar se incorporan una pluralidad de faltas susceptibles de cometerse mediante TICs. Sin embargo, lo dicho hasta el momento, dificílmente sería aplicable a las mismas, pues como tendremos ocasión de ver en la segunda parte de la ponencia, en las faltas no existe la posibilidad solicitar la cesión de los datos identificativos por parte de las operadoras pues esta 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"*. La confusión introducida por la Ley 25/2007 al restringir la posibilidad de

cesión a *la averiguación de delitos graves*[23]. Nos lleva a que una interpretación conforme al concepto de delito grave contenido en el art. 33 CP podría dejar impunes múltiples delitos, ya no digamos faltas disciplinarias, cometidos por Internet o telefonía y 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, por ello la, fundamental, *Circular 1/2013 de la Fiscalía General del Estado de 11 de enero, sobre pautas en relación con la Diligencia de intervención de las comunicaciones telefónicas,* que se explica detenidamente en la segunda parte, mantiene que una interpretación teleológica ha de llevar al entendimiento de que la gravedad debe definirse en atención a las circunstancias concretas del hecho, teniendo en cuenta el bien jurídico protegido y la relevancia social de la actividad, de conformidad con la jurisprudencia recaída en relación con los delitos susceptibles de ser investigados mediante intervenciones telefónicas[24]. 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 impondrá de forma incuestionable autorización del Juez de Instrucción.

Como supuestos especificos de ilícitos informáticos disciplinarios apuntaremos, los recogidos, en la Ley Orgánica 12/2007, de 22 de octubre, del Régimen Disciplinario para la Guardia Civil, 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.*

---

[23] La Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, *sobre conservación de datos generados y tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones*. en su art. 1 también limita el acceso a los datos a la investigación de delitos graves, pero sin definir ni delimitar tal concepto, sino dejando su desarrollo al criterio de los Estados. Limitar el ámbito de la Ley a los delitos graves tal y como se definen en los arts. 13 y 33 CP supondría en realidad frustrar tanto la finalidad perseguida por la Directiva 2006/24/CE como el objetivo de la Convención sobre Ciberdelincuencia del Consejo de Europa, que es precisamente posibilitar la investigación de los delitos que se sirven de las tecnologías de la información y la comunicación.

[24] 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 sólo ha de tenerse en cuenta la gravedad de la pena, sino también su trascendencia y repercusión social (SSTS nº 740/2012, de 10 de octubre, 467/1998, de 3 de abril, 622/1998, de 11 de mayo).

.

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 articulo 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.*

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, del 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 métodos de investigación mas ágiles y eficaces, así como normas procesales y penales 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 mas o menos exclusiva a esta función sino el favorecimiento de una mayor formación en la materia, para que cuando nos encontramos ante un delito cometido mediante TICs, que debemos investigar y como hacerlo, así como hasta donde se puede llegar en la investigación con los medios técnicos existentes y que se puede interesar de los investigadores. Por otra parte la creación de cauces de colaboración con el Fiscal de Sala para la Criminalidad Informática, a fin de contrastar las distintas experiencias estimo que sería, extremadamente, provechosa para el mejor desempeño de nuestra función.

Veo necesario 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 esta a la hora de probar la vinculación del autor al hecho, la prueba que recae sobre TICs 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 aspectos de la conducta típica como su gravedad o la publicidad alcanzada.

La protección jurídico penal de los medios asignados a las Fuerzas Armadas, no puede ser ajena en su regulación, a la importancia de las TICs, para su funcionamiento, pues constituyen el nervio esencial de su operatividad, y, en base, a esa importancia deben ser protegidos tanto de ataques exteriores, como desde el interior por culpa o negligencia.

Por último, y dada la constatación de la cantidad de ilícitos disciplinarios y su trascendencia que se cometen mediante el uso no autorizado de smartphones seria conveniente reflexionar sobre la necesidad o no de que estos dispositivos acompañen al soldado en todo momento de su vida militar, permitiendo una retrasmisión en vivo y en directo de la vida de las unidades, sobre todo en situaciones de conflicto.

BIBLIOGRAFÍA Y LEGISLACIÓN

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, Nº. 9, 2009.

DE LA MATA BARRANCO NORBERTO.J, HERNÁNDEZ DÍAZ LEYRE. "*El delito de daños informáticos: una tipificación defectuosa" Estudios penales y criminológicos,* Nº. 29, 2009, págs. 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, págs. 169-203.

HERNÁNDEZ DÍAZ LEYRE. *"El Delito Informático*", Cuaderno del Instituto Vasco de Criminología, Nº. 23, 2009, págs. 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. D*elitos cometidos a través de Internet. Cuestiones Procesales.* La Ley- Actualidad, 2010.

CIRCULAR 1/2013 DE LA FISCALÍA GENERAL DEL ESTADO, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. Madrid 11 de enero de 2013.

INSTRUCCIÓN 2/2011, sobre el Fiscal de sala de criminalidad informática y las secciones de criminalidad informática de las fiscalías.

INSTRUCCIÓN 10/2011, DE 24 DE FEBRERO, del Secretario de Estado de Defensa, por la que se aprueba la Política de uso de la mensajería interpersonal en la red de área extensa corporativa de propósito general del Ministerio de Defensa (BOD num. 54) de 18 de marzo de 2001.

CONVENIO SOBRE LA CIBERDELINCUENCIA DE 23 DE NOVIEMBRE DE 2001 DEL CONSEJO DE EUROPA; CETS nº 185. España lo firmó el 23 de noviembre de 2001, lo ratificó el 3 de junio de 2010 y entró en vigor el 10 de octubre de 2010.

LEY 25/2007, DE 18 DE OCTUBRE, de Conservación de Datos de las Comunicaciones Electrónicas y a las redes públicas de comunicaciones.

DIRECTIVA 2006/24/CE, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 15 DE MARZO, sobre conservación de datos generados y tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.

LEY 32/2003, DE 3 DE NOVIEMBRE, General de Telecomunicaciones.

LEY *34/2002,* DE 11 DE JULIO, de servicios de la Sociedad de la información y de comercio electrónico