8.2 **Análisis de las diligencias de investigación y procedimientos judiciales incoados y acusaciones formuladas por el Ministerio Fiscal en 2018**

En primer término, ha de recordarse que los datos estadísticos que recogemos en este apartado han sido obtenidos a partir de la información trasladada a la Unidad Central de Criminalidad Informática desde las Fiscalías Provinciales sobre procedimientos judiciales/diligencias de investigación incoados en los distintos territorios por hechos ilícitos competencia de la especialidad, tal y como vienen delimitados en la Instrucción 2/2011 de la FGE. Es decir, se trata de una información que ni coincide ni puede coincidir con los datos recogidos en las estadísticas de los distintos cuerpos policiales, porque, como explicaremos posteriormente con más detalle, la información relativa a atestados o investigaciones en los que no consta autor conocido no está siendo trasladada a los órganos judiciales ni, al menos oficialmente, al Ministerio Fiscal como consecuencia de la interpretación dada al vigente artículo 284 LECrim

Pues bien, según resulta de dicha información, en el año 2018 en el conjunto del Estado se incoaron por estas categorías delictivas un total de 9.069 procedimientos judiciales. Esta cifra implica un incremento en un 35,84 % respecto de los asuntos registrados en 2017, año en el que el volumen de incoaciones ascendió a 6.676. Este aumento interanual, que da cuenta de una tendencia claramente alcista en el volumen de actividades ilícitas cuyo objeto son los datos y/o sistemas informáticos o que se planifican y ejecutan a través de la red, no puede, sin embargo, tomarse como un índice adecuado para valorar la efectiva influencia que el desarrollo tecnológico está teniendo en la delincuencia en sus diversas y múltiples manifestaciones. En ese sentido es llamativo que esa cifra de 9.069 procedimientos incoados en el año 2018 sea muy inferior a la de 22.575 expedientes que se computaron como iniciados en el año 2015 o a la de 20.534 del año 2014, sin que exista razón alguna para afirmar que ese drástico descenso en las últimas anualidades se corresponda con una efectiva reducción de la criminalidad en este ámbito. Más bien al contrario, las estadísticas policiales, y nuestra propia percepción, nos llevan a una conclusión claramente diferente que apunta a un desplazamiento generalizado hacia la red de todo tipo de actividades criminales, dado que el ámbito tecnológico ofrece mayores facilidades para la planificación y ejecución criminal y mejores oportunidades de lograr la impunidad debido, entre otras circunstancias, a las múltiples posibilidades disponibles para

la *anonimización* u ocultación del propio rastro, a la volatilidad de las evidencias y al carácter trasnacional del ciberespacio. Es evidente que estamos asistiendo a un incremento de las actividades delictivas vinculadas al uso de las TIC y esta afirmación se ve avalada por la información facilitada por el Ministerio del Interior, a cuyo tenor las investigaciones por ciberdelitos se incrementaron en un 36 % respecto a 2017 y en un 84 % respecto a 2015, llegando a alcanzar en 2018 la cifra de 110.613.

Como ya hemos explicado detalladamente en memorias anteriores, la razón de ese importante descenso en los últimos años en el volumen de registros judiciales hay que buscarla en la modificación operada en el artículo 284 LECrim por LO 13/2015, de 5 de octubre, que ha determinado que los atestados por hechos ilícitos en los que no conste autor conocido no sean trasladados a los órganos judiciales o al Ministerio Fiscal, a excepción de los supuestos específicos que se citan expresamente en dicho precepto. Por ello, un volumen muy importante de denuncias o diligencias policiales por hechos ilícitos cometidos a través de la red que, por las razones expuestas, no estamos en condiciones de cuantificar, no llegan a conocimiento de los órganos de la Administración de Justicia y por tanto quedan al margen de las estadísticas judiciales y también de las del Ministerio Fiscal que ofrecemos en esta Memoria.

Sin pretender ahondar en el análisis de las consecuencias negativas que, a nuestro entender, genera esta situación, solo nos cabe recordar, por tercer año consecutivo, que una de ellas es la pérdida de información sobre la incidencia, la evolución y las distintas manifestaciones de la delincuencia en la red en orden a valorar la adopción de medidas legislativas u organizativas para afrontar este fenómeno criminal. Dicha disfunción únicamente podría ser paliada con un análisis y estudio conjunto de la información derivada de las innumerables diligencias que quedan almacenadas en las oficinas de denuncia de los distintos cuerpos policiales. En lo que nos atañe más directamente, esa dispersión de información está generando serias dificultades para relacionar entre sí denuncias o actuaciones policiales tramitadas por razón de efectos parciales de una misma actividad criminal que valoradas aisladamente pudieran considerarse no susceptibles de traslado a los órganos de la jurisdicción penal, pero que analizadas conjuntamente permitirían vislumbrar con claridad la acción criminal y sus responsables. Quienes utilizan el ciberespacio para cometer y planificar delitos son conscientes de las ventajas que les aporta esta situación y la aprovechan para intentar dificultar la investigación criminal y facilitar su propia impunidad, por lo que

resulta esencial ofrecer soluciones que permitan solventar los efectos perversos que pueden derivarse de las disfunciones en el tratamiento de dicha información.

La preocupación de esta área de especialización por dicha problemática nos ha llevado a proponer en el Comité Técnico de Policía Judicial algunas medidas para paliar las consecuencias antes mencionadas, que explicaremos con mayor detalle al referirnos a nuestras relaciones con las Fuerzas y Cuerpos de Seguridad. El objetivo de dicha iniciativa es el de prestar nuestra colaboración para hacer posible una actuación eficaz frente a la delincuencia en la red y favorecer, al tiempo, un conocimiento más completo, contrastado y detallado de este fenómeno criminal que permita ir adoptando, con esa finalidad, las decisiones que resulten más oportunas ya sean legislativas, organizativas o de provisión de medios personales y materiales.

Los datos correspondientes a las tipologías delictivas objeto de los procedimientos judiciales incoados en el año 2018, ofrecen el siguiente detalle:

Delitos informáticos		Procedimientos judiciales incoados	%
Contra la libertad	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss)	905	9,98
	Acoso a través de TICs (art 172 ter)	337	3,72
Contra la integridad moral	Trato degradante a través de TICs (art. 173)	65	0,72
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189)	754	8,31
	Acoso menores a través de TICs (art. 183 ter)	127	1,40
	Otros delitos c/libertad sexual a través TIC	326	3,59
Contra la intimidad	Ataques/interceptación sistemas y datos (art. 197 bis y ter)	83	0,92
	Descubrimiento/revelación secretos a través TIC (art. 197)	1-41	4,86
Contra el honor	Calumnias/injurias autoridades a través TIC (art. 215)	162	1,79

Delitos informáticos		Procedimientos judiciales incoados	%
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (arts. 248 y 249)	5.581	61,54
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss.)	25	0,28
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286)	8	0,09
	Delitos de daños informáticos (art. 264, 264 bis y 264 ter)	65	0,72
	Delitos c/ propiedad intelectual a través TIC (arts. 270 y ss.)	37	0,41
De falsedad	Falsificación a través de las TICs	49	0,54
Contra Constitución	Discriminación a través TIC (art. 510)	91	1,00
Otros		13	0,14
Total		9.059	100,00

Como puede apreciarse, el índice más elevado, un 61,54 %, se corresponde con procedimientos cuyo objeto son los delitos de estafa en sus distintas manifestaciones que alcanzaron en números absolutos la cifra de 5.581. Tradicionalmente son los delitos de estafa los que dan lugar anualmente a un mayor número de incoaciones. Así en el año 2017 supusieron un 55,63 % del total de los procedimientos iniciados y en 2016 un 61,35 %. En cifras absolutas, la evolución en el último periodo interanual, desde los 3.715 registros de 2017 a los 5.581 del año memorial, se concreta en un incremento de poco más del 50 %.

Varias son las conclusiones que podemos extraer de estos datos: la primera de ellas es que las conductas típicas encuadrables dentro del delito de estafa sancionado en el artículo 248 CP, son las que en mayor número llegan a conocimiento de los Tribunales o del Ministerio Fiscal de entre las que se cometen a través de las TIC. Ello no quiere decir que sean las que con más frecuencia se cometen en la red porque la cifra oculta de criminalidad en otro tipo de delitos, como la pornografía infantil o los ataques informáticos, resulta por el momento incalculable, pero sin duda son éstos los delitos que con más frecuencia son objeto de denuncia. Y esta es una constante que se viene apreciando desde el año 2012 en que se comenzó el seguimiento estadístico de la ciberdelincuencia. Esta valoración se corrobora con la informa-

ción facilitada al respecto por el Ministerio del Interior, a cuyo tenor el 80 % de las investigaciones por ciberdelitos registrados en 2018 fueron ilícitos de esta naturaleza.

Ahora bien, el porcentaje de expediente judiciales por esta categoría delictiva, respecto del total de los incoados en el marco de actuación de la especialidad, ha descendido considerablemente tras la reforma del artículo 284 LECrim a la que anteriormente hacíamos referencia. Efectivamente, en el año 2015 dicho porcentaje alcanzaba el 80,62 % del conjunto de procedimientos iniciados e incluso llego a superar el 84 % en el año 2014, última anualidad previa a la entrada en vigor de la reforma procesal, es decir, índices en todo caso mucho más elevados que los de las tres últimas anualidades.

Ello nos lleva a la segunda de las conclusiones que obtenemos de este análisis: que las investigaciones por acciones típicas de carácter defraudatorio son las que con mayor frecuencia y en mayor número quedan depositadas en las oficinas de denuncia sin ser trasladadas a los órganos de la jurisdicción penal por considerarse como de autor no conocido. Así, es llamativo que los 18.201 registros efectuados por esta categoría delictiva en 2015 –en que dimos cuenta de la incoación de un total de 22.575 expedientes– se hayan reducido a 5.581 en 2018, casi un 70 % menos, que se concreta en un descenso de 12.620 procedimientos por estos ilícitos. Quiere decirse con ello que la brusca disminución de los procedimientos incoados judicialmente por ciberdelitos entre 2015 y 2018, materializado en 13.506 expedientes, se corresponde en más de un 93 % con denuncias relativas a delitos de estafa en sus diversas manifestaciones.

Estas valoraciones que efectuamos a partir de los datos estadísticos disponibles, son corroboradas por los Delegados provinciales en los informes sobre evolución de la criminalidad en sus respectivos territorios. En ellos, a partir de la información facilitada por los cuerpos policiales, dan cuenta de que un volumen muy elevado de los atestados que se «guardan» en dependencias policiales se refieren a estafas cometidas a través de la red por cuantías aparentemente inferiores a los 400 euros, uso irregular de tarjetas bancarias o utilización fraudulenta de sus numeraciones en operaciones *online* en establecimientos comerciales ubicados en el extranjero. En estos supuestos, la escasa cuantía del perjuicio supuestamente causado, las dificultades anteriormente referidas para interrelacionar los efectos parciales de una misma acción criminal, la propia complejidad técnica de la investigación y la imposibilidad de recurrir para ello a técnicas limitativas de derechos fundamentales o a medidas de cooperación internacional determinan finalmente que dichas actuaciones no sean remitidas a la

jurisdicción penal en el entendimiento de que no es factible la concreción del responsable criminal.

Sin perjuicio de ello y a efectos de la correcta valoración de los datos estadísticos que ofrecemos, es preciso recordar que dentro de este apartado se incluyen una diversidad de actividades delictivas que, aun obedeciendo a dinámicas y planteamientos muy diferentes, se hacen acreedoras de una misma calificación jurídica como delitos de estafa, lo que no obsta a la conveniencia de analizarlas separadamente.

Así, habrán de mencionarse las estafas de carácter más convencional, perfectamente encuadrables en el párrafo 1.º del artículo 248, en cuya ejecución el uso de las TIC constituye el medio idóneo para facilitar la difusión del engaño, aumentar el beneficio ilícito y extender el perjuicio a un número mayor de perjudicados. Nos referimos a la oferta pública fraudulenta de bienes y servicios a través de Internet que suele tener por objeto vehículos de motor, electrodomésticos, dispositivos o elementos informáticos o incluso últimamente entradas a conciertos o espectáculos públicos. Ciertamente cabría plantearse si estos supuestos debieran considerarse incluidos en el marco de actuación de la especialidad tal y como se encuentra definido en la Instrucción nº 2/2011, especialmente cuando se trata de actividades puntuales planificadas y ejecutadas por individuos aislados y con una mínima complejidad técnica, y no faltan, entre los Fiscales Delegados, voces que así lo entienden. No obstante, y aun admitiendo que el tema podría ser cuestionable, ha de dejarse constancia del innegable valor que aporta el trabajo en red a los efectos de garantizar una respuesta eficaz frente a estos comportamientos, a partir de la efectiva coordinación de las distintas diligencias policiales/procedimientos incoados para investigar cada uno de los múltiples efectos derivados de estas conductas.

Además, últimamente se constata que incluso estas actividades ilícitas aparentemente más sencillas en su planificación y ejecución se han venido complicando a medida que las tecnologías iban ofreciendo nuevas y más sofisticadas posibilidades y/o capacidades de actuación. Así, esta misma dinámica delictiva se utiliza por organizaciones criminales, a escala mucho mayor, para la comisión de estafas de gran proyección y, en ocasiones, con dimensión internacional. Buen ejemplo de ello es la investigación, objeto de seguimiento en el expediente de coordinación 7/2018 de la Unidad Central, referida a la compraventa fraudulenta de vehículos a través de páginas web, conocida como *Phishing-car,* en la que se han detectado un total de 118 operaciones simuladas para la supuesta adquisición en el extranjero de vehículos de alta gama con un perjuicio total próximo a los 500.000 euros.

En otros casos el engaño se concreta en ofertas de inversión de alta rentabilidad, en moneda de curso real o virtual e incluso en oro o diamantes, con las que se logra captar la atención de usuarios de la red que, atraídos por la información que se les facilita y las ventajas económicas ofrecidas, hacen llegar a los delincuentes importantes cantidades de dinero que posteriormente no pueden ser recuperadas. Tal es el caso de la actividad desarrollada por quienes, actuando bajo la cobertura de una supuesta entidad denominada Capital Market Bank, han logrado defraudar al menos a 65 personas en todo el territorio nacional por una cuantía superior a los 600.000 euros, lo que ha determinado la incoación del expediente FCI 145/18 (actualmente de coordinación n.º 3/19) de esta Unidad Central de Criminalidad Informática. En relación con este asunto es de interés mencionar que de las denuncias presentadas solo 15 fueron inicialmente trasladadas desde las oficinas de denuncia a los órganos judiciales al considerarse las restantes como de autor desconocido, valoración obviamente condicionada por las dificultades ya comentadas para interrelacionar la información proporcionada por los diversos afectados y que, sin duda, ha favorecido la continuidad temporal de referido proyecto criminal.

En estos y otros supuestos similares, los delincuentes actúan de forma coordinada y con una previa planificación que se ve favorecida por los conocimientos específicos que tienen sobre el funcionamiento del sector de actividad en el que se opera, y también sobre el propio entorno tecnológico, a efectos de hacer posible la utilización de medidas de *anonimización*, ocultación de IPs, apertura de cuentas corrientes bajo identidades supuestas, captación o contratación de mulas, etc. Es decir, ya no se trata simplemente de la utilización de la red como elemento vehicular para difundir el engaño sino, además, de aprovechar sus posibilidades para reforzar y mejorar la planificación y ejecución delictiva, dificultar la investigación y, en definitiva, menoscabar la capacidad del Ministerio Fiscal para dar respuesta penal.

En este último grupo podríamos también incluir las ofertas fraudulentas de servicios tales como alquileres de viviendas de temporada, cada vez más frecuentes en referencia a periodos vacacionales. Son varios los supuestos en que este tipo de conductas, planificadas por grupos criminales, han ido precedidas de ataques informáticos dirigidos contra las agencias especializadas en esa clase de servicios, con el objetivo de apoderarse de información sobre inmuebles disponibles que posteriormente son ofertados, haciendo concurrir de esta forma la actividad defraudatoria con la comisión de delitos de ataque a sistemas informáticos de una u otra tipología.

En relación con estas manifestaciones criminales se ha de poner en valor la labor de impulso y centralización de la información que se está llevando a efecto a través de los expedientes de coordinación incoados en esta Unidad Central, que sumaron 11 en el año 2018. Igualmente estimamos necesario alertar sobre algunas situaciones que se han detectado y suelen aparecer vinculadas a actividades defraudatorias a gran escala que se desarrollan en diversas fases, y cuyos efectos alcanzan en periodos sucesivos a diferentes perjudicados. Así, en este tipo de actividades no es infrecuente que los delincuentes en las etapas ulteriores del *iter criminis* utilicen documentación obtenida mediante engaño de las víctimas estafadas en sus fases iniciales, valiéndose de la misma para usurpar su identidad en los contactos que posteriormente mantienen a través de internet con nuevas víctimas o para abrir cuentas bancarias en las que se depositarán las cantidades que ilícitamente vayan obteniendo. Ello está determinando, como efecto perverso, que quienes han sido víctimas en las fases iniciales del delito figuren en momentos posteriores como presuntos autores/beneficiarios de esas mismas conductas criminales. Para solventar dichas situaciones, el análisis conjunto de la información relacionada con una misma actuación criminal también resulta esencial.

No obstante, muchas dinámicas delictivas vinculadas a las TIC que incluimos en este apartado no encajan en el concepto tradicional de estafa, sino que el desplazamiento patrimonial viene determinado, al menos en parte, por el empleo de manipulaciones informáticas o artificios semejantes (art 248.2 a) CP). Es el caso del *Pharming,* en el que se aprovechan las vulnerabilidades en el software de los servidores DNS *(Domaine Name System*), o en los equipos de los usuarios de Internet para redirigir electrónicamente, por procedimientos de ingeniería informática, un nombre de dominio a otro *sitio* distinto controlado por el atacante y que suele imitar las páginas legítimas, por ejemplo, de entidades bancarias, con el objetivo de captar los datos personales del usuario para su utilización posterior con fines ilícitos. O también del virus troyano conocido como *ransomware* que, en función de parámetros prefijados de navegación web, se activa/ejecuta bloqueando el equipo informático y encriptando su contenido, situación con la que se pretende inducir a la víctima a abonar determinadas cantidades de dinero, ya sea coactivamente o mediante engaño, para recuperar la información perdida.

En los últimos años se utiliza también con frecuencia el llamado *fraude al CEO* o ataque *Business Email Compromiso* (BEC). Esta técnica defraudatoria, dirigida generalmente contra organizaciones empresariales, presenta distintas variantes con un elemento común, la

suplantación de la identidad de directivos, empleados habilitados para gestiones económicas, e incluso de proveedores o clientes en sus comunicaciones electrónicas –una vez obtenida la oportuna información por medios diversos, entre ellos, el acceso irregular a sus dispositivos– para ordenar operaciones económicas aparentemente justificadas en el curso normal de la empresa que permiten desviar importantes cantidades de dinero a cuentas controladas por los delincuentes.

Sin pretensión de exhaustividad, respecto a otras manifestaciones de estafa, no pueden dejarse de mencionar los fraudes de telecomunicaciones o las incontables denuncias por operaciones irregulares utilizando numeraciones de tarjetas de crédito o débito ajenas. En estos casos los datos pueden ser copiados/clonados, bien aprovechando la posesión física de la tarjeta legitima por los delincuentes o sus colaboradores, o bien porque dichos datos se han obtenido por técnicas de *phising, smishing* –suplantación de entidades bancarias en páginas web o mensajes SMS*, hacking o skimming* –instalación de un decodificador invisible en los cajeros automáticos–. Como ya se ha indicado, las dificultades para identificar a los responsables de este tipo de conductas determinan que muchas de las denuncias de este tipo no sean finalmente trasladadas a los órganos de la jurisdicción penal y queden impunes pese a que, año tras año, se incrementa el perjuicio económico derivado de ello.

Los delitos contra la libertad e indemnidad sexual constituyen otro apartado importante de esta Memoria, pues son conductas de extraordinaria gravedad que inciden en bienes jurídicos muy sensibles y cuyas víctimas suelen ser menores de edad y, por tanto, personas extremadamente vulnerables. Estas acciones ilícitas se han visto extraordinariamente favorecidas por las posibilidades que ofrecen las tecnologías para la elaboración y la difusión de todo tipo de contenidos.

A efectos de valorar los datos que se ofrecen, debe precisarse, en primer término, que estas tipologías delictivas no se encuentra afectadas por el limitado régimen de traslado de actuaciones establecido en el vigente artículo 284 LECrim, al hallarse expresamente excepcionadas del mismo, de tal forma que las investigaciones que generan son remitidas a los órganos de la jurisdicción penal aun cuando no conste autor conocido, por lo que la información de la que disponemos constituye un buen reflejo de la actuación policial/judicial en esta materia. No obstante, ello no significa, en modo alguno, que la misma pueda considerarse indicativa de la incidencia real del fenómeno criminal que nos ocupa dado que, hoy por hoy, la cifra oculta de actuaciones ilícitas en este ámbito es incalculable.

Según los datos disponibles, el volumen total de nuevos procedimientos registrados por delitos de este tipo en el año 2018 ascendió a 1.207, un 13,30 % del total de los incoados. De entre ellos 754 se corresponden con delitos de pornografía infantil y/o de personas con discapacidad, 127 con conductas del *child grooming,* acoso a menores de 16 años con fines sexuales, y 326 a otras tipologías contra la libertad sexual de las que también pueden ser víctimas personas mayores de edad. Comparando estos datos con los 1.077 registros del año 2017, se detecta un ligero repunte en la cifra global que, no obstante, se concreta en forma desigual en los resultados parciales. Así descienden en 71 y 32 respectivamente los registros por delitos de pornografía y *child grooming* y se incrementan considerablemente, en 233 apuntes, los correspondientes a otro tipo de delitos contra la libertad sexual cometidos a través de la red.

Como se constata claramente, el número de expedientes incoados por estas tipologías delictivas es muy inferior al de las defraudaciones. La razón de ello hay que buscarla en la circunstancia de que –a diferencia de lo que acontece con las estafas– en la generalidad de estos supuestos, particularmente en los delitos de pornografía infantil, las investigaciones, por razones obvias, no suelen iniciarse por denuncia de los perjudicados sino por actuación de oficio de los cuerpos policiales, ya sea como resultado de actividades de *ciberpatrullaje* en fuentes abiertas, ya por información trasladada por organismos públicos o privados o por fuerzas policiales de otros países que, con ocasión de sus propias investigaciones, detectan direcciones IP ubicadas en España y relacionadas con la distribución de materiales ilícitos. Es por ello que los datos sobre delitos de pornografía infantil se mantienen bastante estables en los distintos periodos anuales. Así, las 581 incoaciones del año 2014 tuvieron un repunte significativo en 2015 para alcanzar la cifra de 767, detectándose un ligero descenso en 2016 con 681 registros y un nuevo incremento en 2017, con 825 registros, que se reducen de nuevo a los 754 del año memorial. Es decir, una cifra media en los cinco últimos años de 722 expedientes, con relativas desviaciones entre uno y otro periodo que fácilmente pueden justificarse en la propia capacidad de actuación de las unidades policiales investigadoras. La mencionada estabilidad en el número de investigaciones/procedimientos tramitados anualmente contrasta con el progresivo incremento de la complejidad de los mismos. Como ya venimos señalando en anteriores ejercicios, los métodos más tradicionales de distribución de pornografía infantil, en cuyo descubrimiento e investigación resulta útil el *ciberpatrullaje* o, incluso, el uso de metabuscadores, se han visto superados por nuevas técnicas de intercambio en la

dark web o mediante sistemas de mensajería instantánea, foros privados o acceso compartido de archivos en la nube. Estos nuevos mecanismos de distribución resultan mucho más difíciles de penetrar, por lo que complican extraordinariamente la investigación haciendo necesaria a dicho fin la utilización de técnicas especiales tales como las operaciones encubiertas o el registro remoto de sistemas, recientemente incorporadas a nuestra norma procesal por la LO 13/2015 de 5 de octubre. Así, podemos citar como ejemplo la investigación –denominada policialmente *Telón de acero*– llevada a efecto el pasado año por la Unidad de Investigación Tecnológica del CNP en coordinación con esta área de especialización y actualmente judicializada, contra una red de distribución de pornografía infantil a través de *Telegram*. Con ocasión de esta intervención se identificaron como integrantes de dicha red a un total de 20 ciudadanos de 12 provincias españolas y se obtuvieron los datos necesarios para la ulterior localización de un número importante de personas, también participantes en la misma red y residentes de otros 41 países, a cuyas autoridades se dio trasladado de la oportuna información a efectos de la prosecución de las correspondientes investigaciones.

Por otra parte, es preocupante la cada vez más habitual detección de actividades de elaboración de material pornográfico en nuestro país. El desarrollo de las tecnologías ha puesto a disposición de la generalidad de los ciudadanos herramientas que permiten la captación de la imagen y del sonido con gran nitidez y perfección, lo que ha determinado que la fabricación de material de estas características pueda hacerse con facilidad con teléfonos móviles o a través de videocámaras en el curso de comunicaciones interpersonales. Es por ello que las investigaciones sobre pornografía infantil en muchas ocasiones aparecen vinculadas a supuestos de abusos y agresiones sexuales o a acciones de *child grooming*, al igual que no son tampoco infrecuentes los supuestos en los que el delincuente se sirve para la elaboración de este material de dispositivos previamente colocados en lugares reservados, tales como baños o vestuarios deportivos, para obtener las imágenes que posteriormente destina a su propio uso o a la distribución a terceros.

En consecuencia, son numerosos los casos de *child grooming* en los que el contacto inicial con el menor de 16 años, con fines de carácter sexual, deviene finalmente en un acto de abuso o agresión concreta o en la obtención efectiva de material pornográfico. Debido a esta circunstancia los resultados estadísticos obtenidos por dicha tipología delictiva, que han descendido en poco más de un 20 % respecto al año 2017, han de valorarse con extrema cautela, dado que en

los supuestos mencionados se generan situaciones concursales de difícil reflejo en nuestras aplicaciones informáticas en las que suele dejarse constancia exclusivamente del delito más grave de entre los diversos cometidos.

Sin duda merecen también una especial atención los atentados contra la libertad y seguridad que se cometen a través de la red, entre los que incluimos las conductas encuadrables en los artículos 169 y ss. y algunas de las sancionadas en el art. 172 ter, ambos del Código Penal. Tal y como resulta de las cifras que ofrecemos en esta Memoria, dichas acciones ilícitas determinaron la incoación de un 13,69 % de los procedimientos judiciales por ciberdelitos registrados en 2018, de los que 905, un 9,98 %, se refieren a delitos de amenazas y coacciones y 337, un 3,72 %, a delitos de acoso permanente. Estos resultados guardan gran similitud con la información ofrecida por el Ministerio del Interior, a cuyo tenor las investigaciones por delitos de amenazas y coacciones supusieron el 10,8 % del total de las realizadas en el año 2018.

La utilización de la red para estos comportamientos ilícitos se ha venido incrementando progresivamente en los últimos ejercicios anuales. Así, en el último periodo interanual, los registros por amenazas y coacciones se elevaron en un llamativo 59 %, lo que ha determinado la recuperación de los índices registrados en los años 2015 y 2016, en los cuales estos ilícitos dieron lugar a 1009 y 989 anotaciones respectivamente. Por su parte el crecimiento es todavía más evidente en referencia al acoso permanente. Desde su incorporación como figura típica al Código Penal por LO 1/2015, los 96 registros del año 2015 fueron elevándose a 131 en 2016 y 200 en 2017 hasta alcanzar en 2018 la cifra de 337.

Esta clara tendencia alcista se explica fácilmente por la profunda penetración de las tecnologías en todos los ámbitos de la actividad humana, lo que está determinando que también se trasladen a la red las propias patologías de las relaciones entre las personas. De esta forma es cada vez más habitual la utilización de la gran diversidad de mecanismos de comunicación de carácter tecnológico disponibles (foros, chats, redes sociales, mensajería instantánea, etc.) para canalizar acciones ilícitas de persecución, hostigamiento o intimidación, en condiciones más favorables en cuanto a la agilidad, seguridad y persistencia de dichas acciones y también en lo que se refiere a las posibilidades que se ofrecen al agresor para ocultar su identidad. Una situación de la que derivan consecuencias especialmente perversas para los colectivos más vulnerables como lo son los menores y las víctimas de violencia de género.

El análisis y valoración de estos comportamientos no puede ni debe hacerse al margen de otro tipo de conductas que también, con frecuencia creciente, estamos detectando en la red y que, participando de unos mismos parámetros, se encuadran, a nuestro entender, en una problemática común. Nos referimos a los delitos contra la integridad moral y también a los atentados contra la intimidad, catalogados estadísticamente como delitos de descubrimiento y revelación de secretos. Los primeros de ellos, generaron 65 anotaciones en el año 2018, cifra casi exacta a las 67 y 69 de los años 2017 y 2016 respectivamente. En esta categoría se incluyen las investigaciones de conductas en las que el agresor a través de la red difunde contenidos con los que se pretende atacar la dignidad o el respeto debido a la persona afectada. En cuanto a las acciones contra la intimidad y los datos de carácter personal en sus diversas manifestaciones, entre las que incluimos la difusión inconsentida de imágenes íntimas sancionada en el artículo 197.7 CP, dieron lugar en su conjunto, en el ejercicio de 2018, a la incoación de 441 procedimientos, un 4,86 % del total, cifra muy próxima, aunque en tendencia inversa, a los 466 registros del año 2017 y a los 404 del año 2016.

Todo este grupo de actividades delictivas de una u otra forma atacan bienes personalísimos y en muchas ocasiones aparecen entremezcladas en su planificación y ejecución en la red, dando lugar frecuentemente a situaciones concursales o, incluso, generando criterios discrepantes acerca de su adecuada tipificación penal. Así ocurre cuando una misma acción criminal lesiona simultáneamente varios derechos tales como la intimidad, la libertad o la integridad moral. Este es el caso, por ejemplo, de la sustracción subrepticia, a través de un dispositivo o sistema, de imágenes de naturaleza íntima que posteriormente son utilizadas para obligar a la víctima a observar determinado comportamiento o para difundir una falsa imagen de la misma que la perjudique o denigre públicamente. Por el contrario, en otros supuestos, la versatilidad de las relaciones humanas y las posibilidades que ofrecen las TIC determinan la aparición de nuevas conductas que, aun capaces de lesionar bienes jurídicos necesitados de protección, no se encuentran tipificadas legalmente. Tal es el caso de la simulación de identidad en la red cuando su finalidad es la denigración o humillación del afectado, sobre cuya necesidad de sanción penal nos hemos pronunciado expresamente en diversas ocasiones.

Antes de finalizar este apartado se ha de mencionar que los expedientes por calumnias e injurias contra autoridades y funcionarios con ocasión de sus funciones –únicos supuestos contra el honor en que

interviene la Fiscalía– determinaron la incoación de 162 procedimientos, un 78 % más que en 2017.

Los procedimientos en los que se investigan ataques informáticos siguen generando resultados de muy escasa entidad. En el año 2018, los expedientes por acceso ilegal a sistemas informáticos o por interceptación o captación irregular de información almacenada o trasmitida por los mismos, dieron lugar únicamente a 83 anotaciones, un 0,92 % del total y los relativos a daños informáticos a 65, un 0,72 % del total. En referencia a ambas tipologías se constata un descenso respecto del año 2017 de muy escasa incidencia en los primeros, al concretarse en 4 registros menos, y de mayor relevancia en cuanto a los daños informáticos que se reducen en casi un 28 %. Igual tendencia se observa respecto de los resultados de 2016, periodo anual en el que se registraron respectivamente 115 y 114 expedientes de las indicadas categorías delictivas. En cierta medida estas cifras son consecuencia de la modificación operada en el régimen de traslado de actuaciones a los órganos de la jurisdicción penal, pues las incuestionables dificultades para la identificación de los responsables de estos ataques provocan que un número no determinado de investigaciones no lleguen a conocimiento de los órganos judiciales ni del Ministerio Fiscal. Pero también influye en estos resultados la conocida resistencia a denunciar dichas agresiones informáticas por parte de las empresas u organizaciones afectadas, con la finalidad de evitar las consecuencias reputacionales que de ello se pudieran derivar.

Sin perjuicio de lo anterior, se llama la atención sobre la importancia de mejorar nuestra capacidad de actuar penalmente frente a estas graves conductas que ponen en riesgo la seguridad de los sistemas y, por ende, el normal funcionamiento de las empresas, organismos e instituciones que de ellos dependen y cuya frecuencia y consecuencias son preocupantes, tal y como se colige de los informes que anualmente elaboran los organismos encargados de la prevención de incidentes de seguridad. Por ello, debe insistirse, una vez más, en la necesidad de establecer, en desarrollo del Real Decreto-ley 12/2018 de 7 de septiembre que incorpora a nuestra legislación la Directiva NIS, un sistema ágil y eficaz que facilite la transmisión de información sobre incidentes de ciberseguridad de naturaleza delictiva desde los organismos administrativos encargados de recibir las correspondientes notificaciones a los órganos y autoridades responsables de la persecución, enjuiciamiento y sanción de dichas conductas.

Los delitos contra la propiedad intelectual generaron 37 nuevos procedimientos en el año 2018, un 0,41 % del total de los incoados. Aunque su volumen es reducido, la complejidad de estas investigacio-

nes hace que se les preste una especial atención siendo todas ellas objeto de seguimiento específico desde la Unidad Central. De entre las que se culminaron en el año 2018 destacamos la que dio lugar a la desarticulación del entramado de direcciones web vinculadas al dominio descargasmix.com, considerada la estructura de piratería más importante en lengua castellana. Esta operación desarrollada por el Departamento de Delitos Telemáticos de la Guardia Civil en colaboración con fuerzas policiales argentinas y con el apoyo y coordinación del área de especialización en criminalidad informática del Ministerio Fiscal español y de la Fiscalía Federal argentina, dio lugar a la realización simultánea de varias entradas y registros en ambos territorios y se saldó con cuatro detenciones, tres en España y una en Argentina y el bloqueo de 49 páginas web.

Al igual que en otras tipologías delictivas, se detecta en los últimos años una clara evolución en las formas de defraudación de los derechos de propiedad intelectual, una de cuyas manifestaciones es precisamente la interceptación y redifusión ilícita de contenidos de televisión sobre IP. En estos casos puede generarse una relación concursal entre los ilícitos sancionados en el artículo 270 del Código Penal y los delitos contra los servicios de radiodifusión e interactivos con consecuencias económicas de mucha entidad. En relación con ello, a finales del año 2018 la Unidad de Investigación Tecnológica del CNP desarrolló una operación de carácter nacional contra establecimientos públicos que, valiéndose de decodificadores preparados fraudulentamente, ofrecían irregularmente a sus clientes retransmisiones deportivas, habiéndose obtenido resultados incriminatorios en 1.106 supuestos. Las consecuencias judiciales de la operación se concretarán en el año 2019.

Finalmente es obligada la referencia a los crímenes de odio, es decir a las conductas que incitan, fomentan, promueven o favorecen la hostilidad, la violencia y la discriminación respecto de los que son diferentes. La preocupación que generan estos comportamientos en el Ministerio Fiscal ha dado lugar a la articulación de una Sección específicamente dedicada a los Delitos de Odio y Discriminación. Sin perjuicio de ello, y como quiera que muchas de estas acciones encuentran en la red una vía ágil y efectiva para su planificación y desarrollo y para la publicitación del *discurso del odio,* también el área de especialización en criminalidad informática, en plena coordinación con aquella, se encuentra activamente implicada en la persecución y enjuiciamiento de estas actividades. Según resulta de los datos estadísticos que ofrecemos, en el año 2018 se incoaron 91 procedimientos judiciales por este tipo de conductas, un 18 % más respecto de los registrados

en el año 2017. Este significativo repunte confirma una tendencia al alza detectada en los últimos cinco años que ha determinado que los 30 registros del año 2014 se elevaran a 40 en 2015, 72 en 2016 y 77 en 2017, hasta alcanzar la cifra de 91 en el año memorial, fruto del esfuerzo volcado en ello tanto por el Ministerio Fiscal como por entidades y asociaciones del sector civil, organismos públicos con responsabilidad en este ámbito y unidades policiales especializadas.

8.2.1 Acusaciones del Ministerio Fiscal

La importancia de los datos que ofrecemos a continuación es incuestionable, pues, a diferencia de los anteriormente analizados, proceden de una fase procesal en la que, una vez culminada la investigación y tras valorar todo el material probatorio obtenido, el Ministerio Fiscal efectúa la calificación jurídica de los hechos y formula su pretensión acusatoria frente a la persona o personas que aparecen como responsables de los mismos. Se trata, por tanto, de información muy depurada y obtenida cuando los contornos de la acción delictiva están claramente definidos, de ahí su valor a efectos del análisis del fenómeno criminal que nos ocupa.

Según la información disponible, en el año 2018 se presentaron un total de 1.955 escritos de acusación por hechos ilícitos encuadrados en el marco de actuación de la especialidad tal y como viene definido por la Instrucción 2/2011 de la FGE. Esta cifra confirma la tendencia alcista que venimos observando desde el año 2012 en que se inició la actividad de esta área de especialización y de cuya evolución dejamos constancia en este sencillo esquema:

Anualidad	2011	2012	2013	2014	2015	2016	2017	2018
Acusaciones	906	1.092	1.262	1.275	1.242	1.648	1.715	1.955

Como puede observarse, el leve descenso en el volumen de acusaciones presentadas en el periodo interanual 2014-2015 constituye simplemente un pequeño paréntesis en un proceso de progresivo incremento, que en el año 2018 se concreta en un índice porcentual del 13,99 % respecto de 2017 y de casi el 116 % en referencia a 2011. Estos datos, analizados conjuntamente con la cifra de sentencias condenatorias en procedimientos del área de especialidad, que sumaron 1.196 en el año memorial, resultan esperanzadores y nos llevan a una valoración, sin duda, positiva. Efectivamente, a nuestro entender, dichos resultados sugieren que se va consolidando la eficacia de la

respuesta jurídico penal ante la delincuencia en la red y aun cuando, tal como hemos expuesto, todavía hay un número importante de investigaciones que son consideradas desde el inicio como impracticables, la actuación seria, eficiente y profesional de los órganos de investigación, persecución penal y enjuiciamiento se concreta cada vez más en resultados positivos.

El detalle de las acusaciones formuladas en atención a las diversas tipologías delictivas es el siguiente:

Delitos informáticos		Calificaciones	%
Contra la libertad	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss.)	305	15,60
	Acoso a través de TICs (art. 172 ter)	108	5,52
Contra la integridad moral	Trato degradante a través de TICs (art. 173)	25	1,28
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189)	425	21,74
	Acoso menores a través de TICs (art. 183 ter)	33	1,69
	Otros delitos c/libertad sexual a través TIC	102	5,22
Contra la intimidad	Ataques/interceptación sistemas y datos (arts. 197 bis y ter)	17	0,87
	Descubrimiento/revelación secretos a través TIC (art. 197)	115	5,88
Contra el honor	Calumnias/injurias autoridades a través TIC (art. 215)	23	1,18
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (arts. 248 y 249)	689	35,24
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss.)	17	0,87
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286)	9	0,46
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	23	1,18
	Delitos c/ propiedad intelectual a través TIC (arts. 270 y ss.)	24	1,23
De falsedad	Falsificación a través de las TICs	20	1,02
Contra la Constitución	Discriminación a través TIC (art. 510)	12	0,61
Otros		8	0,41
Total		1.955	100,00

Al igual que en anteriores anualidades, la cifra más elevada corresponde a las estafas/defraudaciones, que determinaron la presentación de un total de 689 escritos, lo que supone un porcentaje del 35,24 % del total de las elaboradas en el año, y un leve incremento, cifrado en casi un 10 %, respecto de los formulados en 2017 por estas mismas tipologías delictivas.

Siguen en importancia las acusaciones por delitos de pornografía infantil que ascendieron en 2018 a 425, lo que implica un 21,74 % del total y un incremento del 12,4 % de las registradas en 2017. Por su parte, los delitos de *child grooming* dieron lugar a la elaboración de 33 escritos de calificación, 12 menos que en 2017, y los relativos a otros delitos contra la libertad sexual a 102 acusaciones, con un elevado repunte respecto de los 30 del año 2017. Nótese que en esta materia la relación entre el número de acusaciones y el volumen de procedimientos judiciales incoados presenta generalmente índices elevados, lo cual es debido a que las actividades ilícitas investigadas con frecuencia se desarrollan íntegramente en territorio español o, al menos, pueden enjuiciarse en España prescindiendo de otras fases del *iter criminis* planificadas y ejecutadas fuera de nuestro país. Además, la iniciación de oficio de muchos de los procedimientos sobre pornografía infantil suele tener como punto de partida el hallazgo u obtención de información sobre direcciones IP comprometidas en el tratamiento de dichos contenidos, lo que permite identificar con facilidad a los responsables de estas reprobables conductas.

No obstante, esta eficacia se ve afectada negativamente por las importantes carencias en medios personales y materiales de los laboratorios de Policía Científica y Criminalística que están determinando preocupantes retrasos en la emisión de informes periciales cuya incidencia, que alcanza a una pluralidad de tipologías delictivas, repercute especialmente en la tramitación de procedimientos por hechos ilícitos de esta naturaleza.

Por su parte los delitos contra la libertad y seguridad de las personas determinaron la presentación de un total de 413 escritos de acusación, poco más de un 21 % de los elaborados en el año. De entre ellos, 305 lo fueron por delitos de amenazas y/o coacciones, que se incrementan en un 36 % respecto de los del año 2017. Más llamativos son los resultados relativos al delito de acoso permanente, por el que se formularon 108 escritos de conclusiones en el año memorial, con un llamativo incremento del 71,40 % respecto de los 63 calificados en 2017 y de más del 350 % respecto de los 23 del año 2016. En referencia a esta última figura delictiva se constata claramente como el progresivo crecimiento en la incoación de causas judiciales tiene su

reflejo en un acompasado incremento en las acusaciones formuladas por esos concretos ilícitos.

De entre las restantes, destacan las 115 acusaciones por delitos de descubrimiento y revelación de secretos, un 5,88 % del total, ilícitos en los que, a estos efectos, se mantiene una significativa estabilidad con un ligerísimo ascenso, concretado en 5 y 8 escritos de calificación respectivamente, respecto de los elaborados en 2017 y 2016. Similar situación de estabilidad, pero con resultados muy inferiores y, a nuestro entender, claramente alejados de su incidencia real, es predicable de las acusaciones por delitos de daños informáticos que determinaron la elaboración de 23 acusaciones, 2 más que en 2017 y 1 más que en 2016.

Por su parte, los ilícitos contra la propiedad intelectual dieron lugar a la presentación por el Ministerio Fiscal de 24 escritos de calificación, 4 más que en el año precedente, en tanto que respecto de los delitos contra los servicios de radiodifusión e interactivos se formularon 9 acusaciones, 1 menos que en la anterior anualidad.

Finalmente mencionar las 12 acusaciones por delitos de odio/discriminación cometidos a través de la red, registradas en el año memorial, que son reflejo de un ligero descenso respecto de los 17 escritos de calificación presentados en 2017 y los 13 del año 2016.

8.2.2 Diligencias de investigación del Ministerio Fiscal

Ha de recordarse, para quienes no estén familiarizados con estos expedientes, que su nota más característica es que la investigación es asumida directamente por el Ministerio Fiscal. Son actuaciones preprocesales, susceptibles de incoarse de oficio o por denuncia, que se tramitan en base a los arts. 5 del Estatuto Orgánico y 773-2.º LECrim y que están limitadas tanto en su periodo de duración como en el contenido de las diligencias que pueden practicarse, ya que cualquier actuación que implique una intromisión en derechos fundamentales exige necesariamente la judicialización del expediente para recabar la imprescindible autorización judicial.

El número de diligencias de investigación iniciadas en los tres últimos años, que ascienden respectivamente a 316, 346 y 342, es muy superior al de las incoadas en los periodos anuales anteriores a la reforma del artículo 284 LECrim, que no superaban el centenar, como es el caso del año 2015 en el que se registraron únicamente 95 expedientes de este tipo.

Sin duda este incremento deriva del control que se ejerce desde los servicios de criminalidad informática, especialmente en algunos terri-

torios, sobre las denuncias/atestados tramitados en dependencias policiales y no remitidos finalmente a los órganos judiciales en orden a corroborar la oportunidad de dicha decisión. Pero también es la consecuencia de una implicación cada vez mayor de la Fiscalía en la investigación de las conductas que se planifican y ejecutan en la red y que da lugar a que, en no pocas ocasiones, los perjudicados y/o afectados presenten la denuncia directamente ante el Ministerio Fiscal.

También es cada vez más frecuente que las primeras diligencias e investigaciones de hechos ilícitos que presentan una mayor complejidad se trabajen previamente por los Fiscales con las unidades policiales especializadas a través de estos expedientes con el fin de preparar adecuadamente el material probatorio para su aportación al órgano judicial.

Delitos informáticos		Calificaciones	%
Contra la libertad	Amenazas/coacciones a través de TICs (art. 169 y ss. y 172 y ss.)	56	15,60
	Acoso a través de TICs (art. 172 ter)	3	0,88
Contra la integridad moral	Trato degradante a través de TICs (art. 173)	3	0,88
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189)	22	6,43
	Acoso menores a través de TICs (art. 183 ter)	1	0,29
	Otros delitos c/libertad sexual a través TIC	17	4,97
Contra la intimidad	Ataques/interceptación sistemas y datos (art. 197 bis y ter)	5	1,46
	Descubrimiento/revelación secretos a través TIC (art. 197)	26	7,60
Contra el honor	Calumnias/injurias autoridades a través TIC (art. 215)	13	3,80
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (art. 248 y 249)	130	38,01
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss.)	4	1,17
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286)	0	0,00
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	2	0,58
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss.)	6	1,75
De falsedad	Falsificación a través de las TICs	5	1,46

Delitos informáticos		Calificaciones	%
Contra la Constitución	Discriminación a través TIC (art. 510)	49	14,33
Total		342	100,00

Del total de Diligencias de Investigación incoadas en el año 2018, que sumaron 342, la cifra más importante, al igual que en años precedentes, corresponde a las estafas/defraudaciones, con 130 incoaciones, un 38 % del total. Son también muy significativos los datos relativos a la investigación de conductas de amenazas/coacciones que, con 56 registros a los que han de sumarse las 3 correspondientes a investigaciones por acoso permanente, dan cuenta de un incremento superior al 125 % respecto del año precedente y los referentes a delitos de odio y discriminación que dieron lugar a 49 anotaciones, cifra exactamente igual a la del 2017.

Finalmente indicar que del total de las diligencias de investigación incoadas en el año memorial, 194 resultaron finalmente archivadas por no constatarse indicios de acción delictiva, 148 fueron trasladadas a las autoridades judiciales competentes por estimar oportuna la prosecución de la investigación y únicamente 42, un 12 % del total, continuaban en tramitación, a final de año, en alguno de los órganos del Ministerio Fiscal.