8.2 Análisis de las diligencias de investigación y procedimientos judiciales incoados y acusaciones formuladas por el Ministerio Fiscal en 2019

En primer término, es preciso recordar que la información estadística que se recoge en este apartado no es sino la recopilación de los datos facilitados por las fiscalías provinciales sobre los procedimientos judiciales incoados y también sobre las diligencias de investigación registradas y los escritos de acusación presentados por el Ministerio Fiscal por hechos ilícitos competencia de esta área de especialización, tal y como viene delimitada en la Instrucción 2/2011 de la FGE. Pues bien, según resulta de dicha información, en el año 2019 se incoaron en el conjunto del Estado un total de 13.143 procedimientos judiciales por estas categorías delictivas. Dicha cifra supone un incremento del 44,92 % respecto de las incoaciones realizadas en el año 2018, que sumaron 9.069, y de casi el 97 % en referencia a las 6.676 registradas en el año 2017.

Sin duda, estos resultados confirman la tendencia alcista que se viene constatando desde el inicio de la actividad especializada del Ministerio Fiscal en esta materia y que queda reflejada en la información que se ofrece desde entonces. Así, en la Memoria correspondiente al año 2011 se dio cuenta de la incoación de un total de 6.532 procedimientos judiciales por este tipo de ilícitos, cifra que se incrementó en un 21,82 % en 2012, en un 50,64 % en 2013 y en un 71,21 % en 2014, anualidad en la que se alcanzó la suma de 20.534 procedimientos. Ciertamente, la modificación operada en el art. 284 LECrim, por Ley 41/2015 de 5 de octubre, al limitar de forma significativa el volumen de atestados que son trasladados a los órganos de la jurisdicción penal, determinó que nuestras estadísticas reflejaran lo que aparentemente podía parecer una variación en dicha tendencia, concretada, en el propio año 2015, en una ralentización en el volumen de incoaciones que sumaron en ese periodo 22.575 –ligeramente superior en un 9,93 % a las de 2014– y en un brusco cambio de signo en 2016, con un descenso del 64,40 % en el número de registros que no superó los 8.035. Las disfunciones generadas y todavía subsistentes en la interpretación y aplicación del citado precepto –que se comentan en el correspondiente apartado de este texto– dieron lugar a que en el año 2017 siguiera cayendo el número de nuevos procedimientos hasta quedar reducido a 6.676.

Sin embargo, es evidente que dicho descenso no se corresponde con una disminución real de la delincuencia en el entorno virtual,

sino que obedece a la circunstancia de que solo se trasladen a los órganos judiciales y al Ministerio Fiscal aquellos atestados en los que se considere factible la identificación de su autor o en que concurra alguno de los supuestos previstos en el citado art. 284.2.º LECrim. Por el contrario, los indicadores con los que contamos revelan el imparable crecimiento de la actividad delictiva en el ciberespacio, cuyo porcentaje en referencia a la criminalidad tradicional y según datos facilitados por el Ministerio del Interior, ha ido aumentando en forma progresiva y constante, desde un índice del 2,1 % en el año 2011 al 4,6 % en 2016 hasta alcanzar un 9,9 % en 2019, anualidad en que el incremento de investigaciones policiales por ilícitos cometidos en la red respecto del año anterior se cifra en un 35,8 %. Es por ello que, una vez *ajustado* el dato sobre procedimientos judiciales incoados a los nuevos parámetros definidos por el art. 284 LECrim, se ha retomado la tendencia alcista a la que nos referimos, concretándose en el último periodo anual en casi un 45 %.

El análisis cualitativo de la información sobre procedimientos judiciales incoados en el año en atención a las distintas tipologías delictivas ofrece 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.)	961	7,31
	Acoso a través de TICs (art. 172 ter)	420	3,20
Contra la integridad moral	Trato degradante a través de TICs (art. 173)	87	0,66
Contra la libertad ssexual	Pornografía infantil/ discapaces a través de TICs (art. 189)	714	5,43
	Acosos menores a través de TICs (art. 183 ter)	225	1,71
	Otros delitos c/libertad sexual a través TIC	275	2,09
Contra la intimidad	Ataques / interceptación sistemas y datos (art. 197 bis y ter)	84	0,64
	Descubrimiento/ revelación secretos a través TIC (art. 197)	596	4,53

Delitos informáticos		Procedimientos judiciales incoados	%
Contra el honor	Calumnias/ injurias autoridades a través TIC (arts. 215 y ss.)	110	0,84
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (arts. 248 y 249)	8611	65,52
	Descubrimiento secretos empresa a través de TIC (arts. 278 y ss.)	34	0,26
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286)	181	1,38
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	101	0,77
	Delitos c/ propiedad intelectual a través TIC (arts. 270 y ss)	555	4,22
De falsedad	Falsificación a través de las TICs	106	0.81
Contra Constitución	Discriminación a través TIC (art. 510)	83	0,63
Total.....		13.143	100,00

La correcta valoración de esta información exige necesariamente de ciertas precisiones. En primer término, ha de recordarse que los datos que se ofrecen no reflejan, ni pretenden reflejar, la totalidad de la actividad delictiva en el entorno virtual, pues es evidente que un volumen muy importante de ilícitos no llega a conocimiento ni de las Fuerzas y Cuerpos de Seguridad ni de los órganos de la jurisdicción penal o porque no son denunciados o porque no son detectados por los cuerpos policiales en el desempeño de sus labores de prevención de la delincuencia. Es más, la cifra oculta de criminalidad en el ciberespacio es hoy por hoy difícilmente calculable, dada la complejidad y la propia e insondable dimensión del ciberespacio. Pero, además, como ya hemos comentado, por mor de lo dispuesto en el art. 284 LECrim, solamente son trasladados por los cuerpos policiales a los órganos de la jurisdicción penal aquellos atestados en los que la investigación criminal y la determinación de los autores del hecho sea viable, quedando depositadas en las oficinas policiales aquellas actuaciones en las que se entienda no es factible la identificación de sus responsables.

Estas circunstancias condicionan de forma muy significativa los resultados obtenidos, especialmente en algunas tipologías delictivas como el uso fraudulento *online* de numeraciones de tarjetas de crédito

o débito ajenas, en el que la determinación del autor presenta dificultades muy específicas, o los ilícitos relativos a ataques a sistemas informáticos, en los que la denuncia por parte de los afectados es todavía poco frecuente. En consecuencia, es preciso aclarar que algunas de las conclusiones que se expondrán a continuación deben ser valoradas muy cuidadosamente si se pretende su extrapolación al fenómeno de la ciberdelincuencia en su conjunto, ya que se obtienen a partir de resultados claramente condicionados por las limitaciones antes indicadas. A mayor abundamiento, nuestra información adolece de ciertas imprecisiones derivadas de la dificultad para identificar en el registro estadístico inicial el carácter informático de la infracción cuando se trata, por ejemplo, de ilícitos que comparten *nomen iuris* con acciones similares realizadas en un entorno físico o que pueden ser incardinables en varios tipos penales por afectar a una pluralidad de bienes jurídicos, especialmente si alguno de ellos es objeto de atención en otras áreas de especialización del Ministerio Fiscal, como ocurre con los supuestos vinculados a la violencia de género o a los delitos de odio.

Sin perjuicio de las salvedades indicadas, resulta evidente que en el año 2019 la actividad delictiva que dio lugar a un número más elevado de investigaciones judiciales y/o del Ministerio Fiscal fueron las estafas/defraudaciones, que sumaron 8.611 procedimientos judiciales, lo que supone un porcentaje del 65,51 % del total de los incoados en el año memorial. Esta preeminencia viene siendo una constante en la estadística anual, pues debe recordarse que esta misma categoría delictiva ofreció un resultado porcentual del 61,54 % en 2018, 55,63 % en 2017 y 61,35 % en 2016, cifras muy similares pese a la evolución antes referida en el volumen total de incoaciones. Se puede incluso afirmar que el porcentaje real de investigaciones por estafa/defraudación, respecto del total por ciberdelitos, es significativamente superior al reflejado actualmente en las estadísticas de la Fiscalía, afirmación que se basa en dos claros indicadores. El primero de ellos es el resultado obtenido, por este concepto, en nuestro propio sistema de registro en las anualidades previas a la entrada en vigor del actual art. 284 LECrim, a cuyo tenor el porcentaje de procedimientos por estafa fue del 84,39 % y 80,62 % en los años 2014 y 2015 respectivamente. De otro lado son también significativas las cifras que ofrece, al respecto, el Ministerio del Interior, que en 2019 ha fijado en un 88 % el volumen de indagaciones por este tipo de ilícitos respecto del conjunto total de investigaciones que se tramitan anualmente por ciberdelitos. La diferencia entre estos últimos datos porcentuales y los que resultan de la estadística del Ministerio Fiscal en los periodos anuales 2016 a 2019 es consecuencia directa del volumen de denuncias/atestados

policiales por estafas/defraudaciones que no llegan a ser remitidas a los órganos de la jurisdicción penal por la inexistencia de líneas de investigación para la determinación de sus responsables.

Ciertamente, y por todas las razones indicadas, las cifras que se barajan no pueden considerarse un reflejo exacto de la incidencia real de las acciones defraudatorias en el conjunto de la actividad criminal *online*, pero la persistencia en el tiempo de similares resultados permite, cuando menos, dejar constancia no solo de su preocupante frecuencia, sino también de que sin duda son los ilícitos que más habitualmente se denuncian por parte de los ciudadanos. Ahora bien, al valorar estas cifras tampoco ha de olvidarse que bajo la denominación genérica de estafas y defraudaciones se enmarcan una pluralidad de conductas criminales que, aun obedeciendo a dinámicas y planteamientos muy diferentes, se hacen acreedoras de una misma tipificación jurídica en el art. 248 del Código Penal. Por ello, en este apartado concreto se incluyen una gran diversidad de conductas que no obstante comparten un mismo objetivo: la obtención ilícita de un beneficio económico en perjuicio de otro. Lamentablemente, la falta de precisión de los registros informáticos nos impide discriminar estadísticamente unas y otras manifestaciones delictivas, pero al menos a partir de nuestra intervención en este tipo de investigaciones, es posible detallar algunos aspectos esenciales de unas y otras.

Así, en primer término, hemos de referirnos a las estafas de carácter más convencional, sancionadas en el art. 248.1.º CP, en las que el engaño constituye el elemento esencial sobre el que pivota el erróneo desplazamiento patrimonial, y en cuya ejecución el uso de las TIC es un factor dinamizador que contribuye precisamente a facilitar la difusión de ese engaño y, en consecuencia, a extender el perjuicio a un número mayor de víctimas, aumentando el beneficio irregular de los delincuentes. Se trata concretamente de los variados supuestos de ofrecimiento público fraudulento de todo tipo de bienes y servicios a través de páginas *web*, foros o chats que suelen tener por objeto todo tipo de efectos: electrodomésticos, dispositivos o accesorios electrónicos, vehículos de motor e, incluso, ofertas de viajes, alquileres de viviendas de temporada, entradas para conciertos o espectáculos públicos, etc.

En un principio se planteaban como actividades defraudatorias de mínima complejidad y susceptibles de planificarse y ejecutarse por individuos que operaban aisladamente y muchas veces sin especiales habilidades en el uso de las herramientas informáticas. Sin embargo, a medida que los delincuentes han ido perfeccionando la dinámica delictiva y su capacidad de ocultación en la red, sirviéndose de los

diversos mecanismos de anonimización disponibles a dicho fin, estas operaciones defraudatorias se han ido complicando progresivamente. Por ello es cada vez más frecuente que estas actividades se realicen por grupos u organizaciones criminales, en ocasiones de carácter transnacional, que diversifican sus funciones, conocen perfectamente las técnicas y modelos de actuación del sector económico en el que operan y se sirven de la colaboración de intermediarios, vulgarmente conocidos como *mulas*, en las distintas fases del *iter criminis,* circunstancias que dificultan extraordinariamente la investigación y la determinación de los responsables últimos del delito. Como también constituye un factor de complejidad añadido la dispersión geográfica de las víctimas que, aunque no sea buscada de propósito por los criminales, es una consecuencia inherente a las acciones desarrolladas en el ciberespacio y determina inevitablemente que las evidencias del delito se encuentren diseminadas por una pluralidad de territorios.

Además, como ya mencionamos en la memoria anterior y refieren muchos fiscales delegados, no es infrecuente que con ocasión de estas estafas masivas los delincuentes se sirvan, en fases ulteriores de la actividad criminal, de los datos personales o documentación de quienes fueron previamente estafados, de modo tal que utilizan sus identidades para contactar con las futuras víctimas o para abrir las cuentas bancarias en las que han de ingresarse las cantidades fraudulentamente reclamadas. Como consecuencia de ello el perjuicio ocasionado a los afectados se agrava considerablemente, ya que a las pérdidas económicas derivadas directamente de la defraudación sufrida se une el daño moral y, en ocasiones también material, de encontrarse sometidos a la carga de verse involucrados en un número indeterminado de investigaciones criminales en las que figuran como presuntos responsables.

Para solventar dichas situaciones resulta esencial el análisis conjunto de la información relacionada con una misma actuación criminal con el objetivo de orientar de forma centralizada la investigación, coordinar sus resultados en las diferentes jurisdicciones y, si resultara procedente, promover la acumulación de los diversos procedimientos ante el órgano judicial que resulte competente.

Precisamente esa es la finalidad que se pretende con los Expedientes de Coordinación que, con base en la Instrucción 2/2011 de la Fiscalía General del Estado se tramitan desde la Unidad Especializada y que en el año 2019 ascendieron a 7, contando para ello con la colaboración insustituible de los/as fiscales delegados/as, que recopilan y analizan la información de las investigaciones en curso en sus respec-

tivos territorios, y la de los especialistas en investigación tecnológica de los diversos cuerpos policiales.

Igualmente, en los últimos años se han ido generalizando las estafas de inversiones a través de ofertas engañosas de alta rentabilidad, tanto en moneda de curso real como en criptomonedas o criptoactivos con los que se logra captar la atención de usuarios de la red que, atraídos por la información que se les facilita y las ventajas económicas prometidas, transfieren a los delincuentes importantes cantidades de dinero que posteriormente no pueden ser recuperadas. Algunos fiscales delegados alertan acerca de los supuestos en los que los defraudadores plantean la operación de forma tal que los perjudicados han de remitir sus aportaciones directamente a los *exchanger,* muchas veces radicados en el extranjero, circunstancia que complica en mayor medida la identificación de los responsables criminales. Por ello, cada vez resulta más necesario establecer mecanismos legales que hagan posible la obtención de información de los proveedores de servicios de cambio de monedas virtuales y de custodia de monederos electrónicos, posibilidad que sin duda se verá favorecida con la implementación en el ordenamiento jurídico español de la *Directiva (UE) 2018/843, de 30 de mayo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo.*

Junto a estas actividades que, aun adaptadas a las peculiaridades del medio de comisión, se enmarcan fácilmente en el concepto de la estafa tradicional, incluimos en este apartado relativo a las defraudaciones otras muchas dinámicas delictivas en las que el desplazamiento patrimonial viene determinado, al menos en parte, por el empleo de manipulaciones informáticas y que encuentran su adecuada tipificación en el art. 248-2.º a) CP. Tal es el caso del *pharming*, técnica en la que los delincuentes aprovechan las vulnerabilidades en el *software* de los servidores DNS *(Domaine Name System*) o en los equipos de los propios usuarios, para redirigir electrónicamente y por procedimientos de ingeniería informática, un nombre de dominio a otro *sitio* distinto controlado por el atacante y en el que, generalmente, se imitan páginas legítimas de instituciones oficiales o entidades bancarias con el objetivo de captar los datos personales de la víctima para su utilización posterior con fines ilícitos. En estos casos la introducción por el perjudicado de sus datos en una página falsa no deriva propiamente de un razonamiento mental erróneo de la víctima motivado por el engaño de otro, sino de la manipulación informática del sistema, que redirige la petición correctamente efectuada a un sitio web simulado *(spoofed bank web sites)* por el delincuente.

En otros casos, el desplazamiento patrimonial se logra combinando el engaño con la manipulación informática, como en el *phising* o en los casos conocidos como *estafa del soporte técnico*, que han dado lugar en el año 2019 a la tramitación de diversos procedimientos judiciales. En estos últimos supuestos, mediante una intrusión irregular –normalmente un *malware* adjunto a un *link* o a un correo electrónico malicioso– el atacante provoca que en el dispositivo de la víctima aparezca una advertencia de mal funcionamiento acompañada del consejo de contactar con el equipo técnico correspondiente a cuyo fin se facilitan los datos necesarios para ello. Una vez la víctima establece el contacto sugerido, los delincuentes, simulando el ejercicio de dicha función y con el fingido pretexto de hacer la oportuna reparación, toman el control del sistema, lo que les permite llevar a efecto sus objetivos, ya sea obtener cantidades indebidas por simuladas reparaciones, *exfiltrar* información de interés o cualquier otro que estimen oportuno. Esta mecánica delictiva está siendo utilizada por grupos organizados de carácter transnacional y, aun cuando el perjuicio individualmente ocasionado no suele resultar muy elevado, ha generado un volumen muy importante de denuncias. Una investigación por hechos de estas características dio lugar a la incoación, en 2019, de uno de los expedientes de coordinación tramitados por la Unidad Especializada, lo que permitió recopilar más de 130 denuncias, gran parte de las cuales no habían sido trasladadas a los órganos de la jurisdicción penal en razón a lo establecido en el art. 284 LECrim, antes citado. Dicho expediente de coordinación ha dado lugar a las Diligencias Previas n.º 10/2018 del Juzgado n.º 1 de Calatayud, actualmente en tramitación.

Esa misma mezcla de engaño y manipulación informática se utiliza en el llamado *fraude al CEO* o en el ataque *Business Email Compromiso* (BEC). Estas técnicas, dirigidas generalmente contra organizaciones empresariales, presentan distintas variantes con un elemento común: la suplantación de la identidad de sus directivos, representantes, empleados habilitados para gestiones económicas e incluso de proveedores o clientes. Una vez los delincuentes obtienen la información necesaria sobre el funcionamiento de la empresa –a través de diversos medios, entre ellos el uso de técnicas de ingeniería social o el acceso irregular a sus sistemas informáticos–, ordenan por medios electrónicos operaciones económicas aparentemente justificadas en el tráfico comercial ordinario de la entidad perjudicada, a cuyo fin utilizan fraudulentamente los datos personales de quien tiene atribuciones para adoptar dichas decisiones, desviando de esta forma importantes cantidades de dinero en su beneficio.

En este breve repaso de las actuaciones fraudulentas *online*, realizado sin pretensión alguna de exhaustividad, no se pueden dejar de mencionar los fraudes en las telecomunicaciones o las numerosísimas denuncias presentadas por operaciones de utilización irregular en la red de numeraciones de tarjetas de crédito o débito ajenas. A esos efectos, los datos pueden ser copiados/clonados por técnicas de *skimming*, aprovechando la posesión física de la tarjeta legítima por los delincuentes o sus colaboradores –empleados o trabajadores de establecimientos públicos de todo tipo– o a través de la instalación de un decodificador invisible en los cajeros automáticos, o también mediante *phising, smishing* –suplantación de entidades bancarias en páginas web o mensajes SMS– *hacking,* etc. Las dificultades para identificar a los responsables de estas conductas determinan que muchas de las denuncias no sean trasladadas a los órganos judiciales y al Ministerio Fiscal, en razón al art. 284 LECrim y engrosen el número de las que quedan depositadas en las oficinas policiales.

Una variante de estas ilícitas actividades que está generando justificada preocupación por su incremento en el último periodo anual, es la que se conoce como *SIM Swapping*. En estos casos los delincuentes tratan de burlar el doble factor de autentificación (2FA) establecido por las entidades bancarias para proteger las transacciones electrónicas de sus clientes, accediendo de forma irregular a los códigos alfanuméricos de confirmación, de uso único, generados con ocasión de cada una de las transacciones. Como quiera que dichos códigos se comunican al usuario de la banca *online* a través de un mensaje SMS, enviado su dispositivo móvil, la técnica empleada es la obtención irregular, con carácter previo, de un duplicado o una nueva tarjeta SIM a nombre de la víctima –normalmente usurpando su identidad para solicitarla del operador de telefonía correspondiente– que el atacante inserta en un terminal bajo su control, provocando el bloqueo la tarjeta original. De esta forma, el delincuente se garantiza la recepción en su dispositivo del código de confirmación correspondiente a la transacción fraudulenta y, en definitiva, la posibilidad de hacer efectiva la misma en su propio beneficio.

El volumen de procedimientos por delitos contra la libertad y seguridad de las personas cometidos a través de las TIC es también muy relevante. Ascienden en conjunto a 1.381, un 10,50 % del total de las incoaciones por ciberdelitos, de los que 961 tuvieron su origen en denuncias por amenazas y/o coacciones y 420 por conductas de acoso permanente. Aunque su incidencia en los datos globales es muy inferior a la de las estafas, su relevancia va aumentando de año en año, especialmente en lo que se refiere a los supuestos de acoso perma-

nente que se han incrementado en más de un 24 % respecto de los 337 expedientes registrados en 2018 y en un 110 % en atención los 200 incoados en 2017. La afectación de estos comportamientos a bienes jurídicos de carácter personalísimo y la circunstancia de que con frecuencia se manifiesten entre menores de edad o en el marco de la violencia de género, determina la especial preocupación que estas acciones están generando en ámbitos nacionales e internacionales y los trabajos en curso para articular mecanismos legales que permitan actuar eficazmente contra sus responsables, protegiendo al tiempo los intereses y derechos de las víctimas. Esa misma preocupación ha determinado que la Fiscalía General del Estado haya estimado conveniente analizar de forma específica esta materia en un capítulo independiente de esta misma memoria, al que nos remitimos, para un estudio más pormenorizado de los problemas relativos a la investigación, persecución y enjuiciamiento de estas conductas.

Por su parte, los delitos contra la libertad e indemnidad sexual constituyen otro apartado de especial interés pues, no en vano, son conductas extremadamente graves y peligrosas que afectan a bienes jurídicos muy sensibles y en las que frecuentemente –en muchos casos, por exigencia del tipo penal– los perjudicados son personas menores de edad que como consecuencia de la agresión pueden resultar seriamente perturbadas en su normal desarrollo y evolución personal. Lamentablemente, se trata de acciones cuya planificación y ejecución se ha visto favorecida por la utilización de las TIC para el contacto interpersonal y la elaboración y la difusión de todo tipo de contenidos.

Como resulta de la estadística, en el año 2019 se incoaron un total de 1.214 procedimientos judiciales por hechos ilícitos cometidos a través de la red encuadrables en este apartado, integrando un 9,23 % del total de los registrados en el año. De entre ellos 714 tuvieron por objeto conductas relativas a la elaboración, distribución o posesión de material pornográfico infantil; 225 se referían a acciones de *child grooming* y 275 a cualquier otra acción *online* contra estos mismos bienes jurídicos. Estos datos, globalmente considerados, son muy similares a los del año 2018 en el que se incoaron 1.207 procedimientos de este tipo. El análisis detallado de los mismos revela un ligero descenso, en poco más de un 5 % en los relativos a pornografía infantil, un notable ascenso, en un 77 %, respecto al *child grooming* y una reducción, del 15,64 %, en los correspondientes a otras figuras contra la libertad sexual.

Es especialmente significativa, por tanto, la tendencia al alza en las investigaciones sobre acoso sexual a menores que, con algún leve descenso, aumentan de forma progresiva en el último quinquenio: 98

incoaciones en los años 2015 y 2016; 159 en 2017; 127 en 2018 y 225 en la última anualidad. Por su parte los procedimientos sobre pornografía infantil mantienen una incidencia bastante estable en los últimos cinco años con leves alteraciones al alza o a la baja, a excepción del periodo interanual 2016-2017, según se colige de las siguientes cifras: 767 en el año 2015; 681 en 2016; 825 en 2017; 754 en 2018 y 714 en 2019.

Estos resultados, en términos generales, constituyen un reflejo adecuado de la efectiva actuación policial/judicial en este ámbito, dado que las investigaciones por estos ilícitos se encuentran exceptuadas del régimen general del art. 284 LECrim y, en consecuencia, han de remitirse a los órganos de la jurisdicción penal aun cuando no sea factible la determinación de su autor. Ahora bien, su correcta valoración ha de hacerse sin olvidar que este tipo de indagaciones, particularmente las relativas a la distribución pornografía infantil y también en muchos casos las que se refieren a la elaboración de dicho material, no provienen normalmente de denuncias presentadas por los propios perjudicados, sino de la labor de *ciberpatrullaje* de los investigadores o también de la información remitida por cuerpos policiales de otros países, organismos nacionales o internacionales –como el *Nacional Center for Missing and Exploited Children* (NCMEC)– o incluso por ciudadanos particulares que detectan contendidos pedófilos con ocasión de su navegación por la red. Es decir, en materia de pornografía infantil, las cifras que se ofrecen no reflejan en absoluto el volumen e importancia de los delitos de esta clase cometidos en la red sino, únicamente, las investigaciones en curso iniciadas por los cuerpos policiales, generalmente de oficio, a partir de la información obtenida y condicionadas inevitablemente, en su número y alcance, por los medios personales y materiales de los que disponen. Ello explica qué pese a los esfuerzos de las unidades policiales especializadas, el número de expedientes por estos tipos ilícitos se mantenga de una forma relativamente estable al margen de la evolución real de estas manifestaciones criminales.

Pues bien, estas circunstancias, poco favorables a una actuación realmente efectiva frente a este peligrosísimo fenómeno criminal, se agravan considerablemente por la complejidad creciente de las indagaciones como consecuencia de la utilización por los delincuentes de mecanismos cada vez más sofisticados para el intercambio y distribución del material pedófilo. Así, es frecuente que el tráfico de estos contenidos se lleve a efecto en foros ocultos en la *dark web* o mediante sistemas de mensajería instantánea como *Telegram* o *Whatsapp,* o incluso compartiendo archivos almacenados en la nube, lo que obliga

a hacer uso de técnicas especiales de investigación como las operaciones encubiertas o el registro remoto de sistemas.

Además, la potencialidad de los utensilios tecnológicos está favoreciendo extraordinariamente no solo la distribución masiva sino también la preparación de contenidos pedófilos pues, no en vano, los dispositivos informáticos, fijos o móviles, están dotados de videocámaras o instrumentos de grabación de alta definición que hacen posible la captación de imágenes de abuso y/o de carácter pornográfico en cualquier lugar y ocasión. La consecuencia de ello es la detección cada vez más habitual en nuestro país de conductas incardinables en el art. 189.1.º a) CP, en muchos casos vinculadas a acciones previas de *child grooming.* Buen ejemplo de ello es el Sumario n.º 14/2017 del Juzgado de Instrucción n.º 3 de Tortosa, seguido contra siete personas que, actuando coordinadamente, durante un prolongado periodo de tiempo, contactaron con más de un centenar de menores de edad en diversos puntos del territorio nacional y ocasionalmente fuera de nuestras fronteras, para utilizarlos en la elaboración de material pornográfico que luego distribuían junto con otros contenidos de similar naturaleza, llegando a abusar sexualmente de algunos de los menores con esa misma finalidad. Presentado escrito de acusación por el Ministerio Fiscal por delitos de elaboración y difusión de material pornográfico, abuso sexual y organización criminal, el juicio oral se celebró en el mes de noviembre del pasado año, respecto de cuatro de los acusados –al encontrarse los demás en rebeldía– habiéndose dictado sentencia condenatoria en el mes de marzo de la anualidad en curso.

Otra manifestación importante de la ciberdelincuencia son los ataques a los sistemas de información que, como es conocido, nuestro legislador ha tipificado en dos apartados distintos del Código Penal, en atención al bien jurídico protegido: los delitos de descubrimiento y revelación de secretos y los de daños informáticos. En cuanto a los primeros, sancionados en los arts. 197 bis y ter CP, dieron lugar a la incoación de 84 procedimientos en el año 2019, cifra muy similar a la de 2018 y ligeramente inferior a los 87 registrados en 2017. Son comportamientos que se encuentran vinculados generalmente a otras figuras delictivas, como los delitos contra la intimidad del art. 197 1.º y 2.º o los de descubrimiento y revelación de secretos de empresa del art. 278 todos del CP, dado que el acceso irregular a sistemas o la interceptación de transmisiones suele tener como objetivo la exfiltración de información de una u otra naturaleza. En muchos de estos supuestos en los que son de aplicación normas concursales, no es extraño que únicamente quede constancia

a efectos estadísticos del atentado contra la intimidad, los datos personales o los secretos de empresa, obviándose la información sobre la intromisión informática como mecanismos de ejecución, lo que puede explicar el reducido número de registros por conductas del art. 197 bis que contrasta con los 596 relativos a delitos del artículo 197 en sus distintas modalidades. El análisis detallado de estos últimos, cuyo incremento en el último año ha sido de más del 35 % respecto de los 441 procedimientos incoados en año 2018, se efectúa en el capítulo de esta memoria dedicado al tema de tratamiento específico, al que nos remitimos a esos efectos.

Respecto de los ataques de sabotaje informático, tipificados como daños en los arts. 264, 264 bis y 264 ter CP, determinaron la incoación de 101 procedimientos judiciales en el año 2019, reflejo de un claro repunte de más del 55 % respecto de los 65 registrados en 2018 y de un 12,2 % respecto de los 90 del año 2017. Aunque todavía de forma tímida, va aumentando progresivamente el número de investigaciones criminales por dichas manifestaciones de agresión informática que tan gravemente afectan a la seguridad digital y que todavía, en muchas ocasiones, no llegan a ser denunciadas por múltiples razones, entre ellas el perjuicio que a efectos reputacionales pudiera derivarse del conocimiento público de las vulnerabilidades de la entidad u organismo atacado. En 2019 han adquirido una especial preeminencia las agresiones a través del virus *ransomware*, cuyo efecto es la encriptación del sistema afectado impidiendo a su titular el acceso a la información almacenada en el mismo. Según el informe IOCTA 2019 de Europol *sobre evaluación de amenazas vinculadas al crimen organizado en Internet* estas acciones con *ransomware* son las más comunes y dañinas en términos económicos, pues los perjuicios que generan pueden llegar a ser elevadísimos. Concretamente en los últimos meses del año memorial se produjeron ataques de esta naturaleza contra diversas entidades públicas y privadas de nuestro país usando la variante *ryuk* del citado virus, lo que ha dado lugar a la apertura de las correspondientes investigaciones criminales actualmente en curso, situación que podría reproducirse en el presente año a tenor de las previsiones de organismos tales como CCN-Cert y CNPIC que advierten de campañas utilizando este mismo virus probablemente dirigidas al sector financiero.

Los delitos contra la propiedad intelectual dieron lugar en 2019 a la incoación de 555 procedimientos, reflejo de un extraordinario crecimiento respecto de los 37 registros por ilícitos de esta naturaleza en la anualidad precedente. Casi todos ellos derivan de la operación realizada finales de 2018, previa denuncia de la Liga Profesional de

Fútbol, por la Unidad de Investigación Tecnológica del CNP contra los titulares de 1.106 establecimientos públicos de todo el territorio nacional que, valiéndose de decodificadores preparados fraudulentamente, ofrecían irregularmente a sus clientes retransmisiones deportivas de difusión limitada y que han dado lugar a la incoación del importante volumen de actuaciones judiciales que refleja la estadística. La tipificación jurídica de dichas conductas como delitos contra la propiedad intelectual del art. 270 del CP y/o como delitos contra los servicios de radiodifusión e interactivos del art. 286 del mismo texto penal y la relación concursal aplicable entre ambas figuras, han dado lugar a un intenso debate jurídico-doctrinal hasta el momento no plenamente resuelto. Esta circunstancia explica también el alto número de registros por delitos contra los servicios de radiodifusión e interactivos que ascienden a 181 en 2019 frente a los 8 procedimientos de 2018.

Finalmente han de reseñarse los 83 procedimientos por conductas incardinables en el art. 510 del CP. Se trata de investigaciones que tienen por objeto las actividades que incitan, fomentan, promueven o favorecen la hostilidad, la violencia y la discriminación respecto de los que son diferentes. Aun cuando en el seno de la Institución existe una Sección específicamente dedicada a los Delitos de Odio y Discriminación, como quiera que muchas de estas conductas se planifican y ejecutan a través de la red como vía ágil y efectiva 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 investigación, persecución y enjuiciamiento de estas conductas. Los 83 procedimientos registrados en el año 2019 suponen un ligerísimo descenso de un 8,7 % respecto de los incoados en 2018 lo que, a nuestro entender, no altera en lo esencial la tendencia alcista que en este ámbito se viene observando desde el año 2014, en el que se anotaron 30 nuevos procedimientos de esta naturaleza y que tuvo su punto álgido en los 91 registros del año 2018. La preocupación generada por el uso frecuente de las TIC para la difusión de esta clase de contenidos y su perversa incidencia en el respeto debido a los derechos y libertades fundamentales de las personas, se ha concretado en nuestro país en la articulación de unidades especializadas en esta materia, no solo en los cuerpos policiales sino también en el Ministerio Fiscal, que dedica a este tema importantes esfuerzos de los que da cuenta la publicación de la Circular 7/2019 de 14 de mayo. Todo ello junto con los trabajos en curso en la Comisión de Seguimiento del Convenio Interinstitucional contra el Racismo, la

Xenofobia y otras formas de Intolerancia, que integra a diversos departamentos ministeriales y otros organismos e instituciones, y en la que Fiscalía desempeña una activa labor que está determinando una actuación cada vez más efectiva frente a estos graves comportamientos.

8.2.1 Acusaciones del Ministerio Fiscal

Los datos relativos a los escritos de acusación formulados por el Ministerio Fiscal tienen un valor muy especial porque son reflejo de aquellas investigaciones en las que ha sido posible obtener resultados efectivos tanto en el esclarecimiento de las acciones ilícitas planificadas y/o ejecutadas a través de la red, como en la determinación de la personas o personas responsables de las mismas. Además, el escrito de calificación de la Fiscalía, por su propia naturaleza y finalidad, ofrece una reseña detallada de los hechos supuestamente acaecidos, concienzudamente depurados en la fase de instrucción, junto con una tipificación penal muy definida de acuerdo con criterios técnico-jurídicos altamente cualificados. Es por ello que los datos que se ofrecen en este apartado resultan mucho más precisos y ajustados a la realidad que los relativos al volumen de procedimientos incoados, ya que estos últimos se obtienen en una fase muy preliminar de la investigación, cuando todavía no se encuentran claramente definidos los contornos de la actividad ilícita, por lo que pueden verse posteriormente desvirtuados o modificados.

Según la información obtenida de las fiscalías provinciales, en el año 2019 se presentaron por la Institución un total de 2.847 escritos de acusación por delitos incluidos en el marco de la especialidad definido por la Instrucción 2/2011 de la FGE. Esta cifra confirma la tendencia al alza que se viene observando desde el año 2012, ejercicio en que se inició la actividad como tal de este área de especialización, y cuya evolución es la siguiente:

Anualidad	2011	2012	2013	2014	2015	2016	2017	2018	2019
Acusaciones	906	1.092	1.262	1.275	1.242	1.648	1.715	1.955	2.847

El número de escritos de acusación presentados en el año memorial refleja un incremento de casi el 46 % respecto de los formulados en 2018 –cifra muy significativa si la comparamos con los índices del 13,9 % y del 4 % detectados respectivamente, por igual con-

cepto, en los periodos interanuales 2017-2018 y 2016-2017– y que coincide en gran medida con el repunte en el volumen de procedimientos incoados en 2019 que, como indicamos, es del 44,92 %. En ello ha influido, sin duda, la circunstancia de que únicamente sean trasladadas a la autoridad judicial y al Ministerio Fiscal las investigaciones en las que es posible la identificación del responsable de la acción ilícita y, por tanto, resulta factible concretar el ejercicio de la acción penal en personas determinadas, pero, además, estos resultados son, ante todo, la consecuencia derivada de una mayor eficacia en la actuación tanto de los investigadores policiales como de los órganos de la jurisdicción penal y, por ende, de una más adecuada respuesta desde el Estado de Derecho ante este peligroso fenómeno criminal.

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.)	295	10,36
	Acoso a través de TICs (art. 172 ter)	196	6,88
Contra la integridad moral	Trato degradante a través de TICs (art. 173)	55	1,93
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189)	372	13,07
	Acosos menores a través de TICs (art. 183 ter)	90	3,16
	Otros delitos c/libertad sexual a través TIC	100	3,51
Contra la intimidad	Ataques / interceptación sistemas y datos (art. 197 bis y ter)	17	0,60
	Descubrimiento/ revelación secretos a través TIC (art. 197)	188	6,60
Contra el honor	Calumnias/ injurias autoridades a través TIC (arts. 215 y ss.)	11	0,39

Delitos informáticos		Calificaciones	%
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (arts. 248 y 249)	1132	39,76
	Descubrimiento secretos empresa a través de TIC (arts. 278 y ss.)	18	0,63
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286)	83	2,92
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	24	0,84
	Delitos c/ propiedad intelectual a través TIC (arts. 270 y ss.)	190	6,67
De falsedad	Falsificación a través de las TICs	62	2,18
Contra Constitución	Discriminación a través TIC (art. 510)	14	0,49
Total.....		2.847	100,00

La cifra más elevada, como venía siendo habitual en años anteriores, corresponde a los procedimientos por estafa y/o defraudación, que dieron lugar a la presentación de un total de 1.132 escritos de acusación, lo que supone casi un 40 % del total de los formulados en 2019 y un incremento de más del 64 % respecto de las 689 acusaciones elaboradas en 2018 por estas mismas tipologías delictivas. La relación entre el número de escritos de acusación y el volumen de procedimientos incoados en el año por estos ilícitos (8.611) ofrece un índice del 13,15 %, dato que debe valorarse con cautela porque no existe una correlación absoluta en los términos de la comparación, pues solo una parte de los procedimientos incoados en un único periodo anual son calificados en esa misma anualidad, lo que no impide sirva para corroborar esa mejora en la eficacia a la que antes aludíamos, si tenemos en cuenta que esa misma comparación ofreció en el año 2018 un índice del 12,41 %.

Siguen en importancia, aunque con resultados muy inferiores, las acusaciones formuladas por delitos de pornografía infantil que sumaron 372, lo que constituye un 13 % del total general y un sensible descenso, cifrado en un 12,47 % de las computadas en 2018. Este resultado que, al menos en parte, se explica en el menor volumen de expedientes judiciales incoados por estas figuras típicas en 2019, a nuestro entender ha podido también venir determinado por la complejidad creciente de las investigaciones de esta clase de ilícitos a la que anteriormente se hacía referencia, que dificultan la concreción de los hechos y la determinación de sus autores, así como por la falta de medios personales y materiales tanto de las unidades policiales espe-

cializadas como de los laboratorios de criminalística y policía científica que en este último caso, como ya hemos tenido ocasión de poner de manifiesto en anteriores memorias, están generando retrasos en la emisión de informes periciales.

Por el contrario, los escritos de acusación por delitos de *child grooming* reflejan un importante repunte de más del 172 %, ya que se alcanzó la cifra de 90 frente a los 33 formulados en el año 2018, lo que se corresponde con un claro aumento, aunque no tan llamativo, en el volumen de procedimientos incoados por esta clase de delitos.

Los ataques contra los sistemas informáticos sancionados en los arts. 197 bis y ter CP dieron lugar a 17 escritos de acusación, cifra exactamente igual a la de 2018, si bien recordemos que dichas conductas en muchas ocasiones suelen aparecer asociadas a delitos contra la intimidad, los datos personales o aquellos relativos al descubrimiento de secretos de empresa, por lo que su reflejo estadístico puede quedar enmascarado en esas otras figuras típicas que, a su vez, generaron 188 y 18 escritos de acusación respectivamente.

En cuanto a las acusaciones por actos de sabotaje informático tipificadas en los arts. 264, 264 bis y 264 ter CP, sumaron en el año 2019 un total de 24, cifra levísimamente superior a los 23 del año 2018, a los 21 de 2017 y a los 22 del año 2016. La estabilidad en estos datos y el leve incremento en la incoación de nuevos procedimientos por delitos de esta naturaleza, pese a la frecuencia creciente de las agresiones a sistemas y elementos informáticos, deja constancia de que la respuesta penal ante este tipo de conductas resulta todavía insuficiente y necesita ser mejorada.

Por su parte, los escritos de acusación por ilícitos contra la propiedad intelectual ascendieron en el año memorial a 190, un aumento de casi un 700 % respecto de los 24 presentados en 2018. La explicación de este altísimo repunte está en la operación antes comentada desarrollada a finales de 2018 por el Cuerpo Nacional de Policía contra un número muy elevado de establecimientos públicos por la difusión no autorizada de contenidos protegidos. Esta circunstancia justifica igualmente el incremento de más del 800 % en el número de escritos de acusación por delitos contra los servicios de radiodifusión e interactivos, que alcanzaron en 2019 la cifra de 83 frente a los 9 presentados en 2018.

También han de mencionarse en este apartado las 14 acusaciones por delitos de odio y/o discriminación presentadas en 2019, que superan levemente las 12 del año precedente, aunque sin alcanzar la cifra de 17 que se registró en 2017.

8.2.2 Diligencias de investigación del Ministerio Fiscal

La peculiaridad de estos expedientes es que son iniciados y tramitados por el Ministerio Fiscal, que es quien dirige directamente la investigación. Se trata de actuaciones preprocesales que pueden incoarse de oficio o por denuncia de terceros, al amparo de lo dispuesto en los arts. 5 del Estatuto Orgánico y 773.2.º LECrim, diligencias que se encuentran limitadas en un doble sentido: en su periodo de duración, que no puede exceder de seis meses o excepcionalmente de un año, sin perjuicio de la posibilidad de ulterior prórroga, y en el alcance de la actuación investigadora, al encontrase vedadas a la Fiscalía aquellas actuaciones que impliquen una intromisión en derechos fundamentales, para cuya práctica deberá solicitarse autorización judicial, lo que necesariamente dará lugar a la judicialización de las actuaciones.

Estos expedientes son sin duda alguna un claro reflejo de la implicación activa de la propia Fiscalía en el esclarecimiento de los hechos delictivos que llegan directamente a su conocimiento. En ocasiones, mediante el traslado de información por parte de los cuerpos policiales que, cada vez con más frecuencia, dan cuenta de sus investigaciones a los integrantes del área de especialización, buscando el apoyo y la dirección jurídica que garantice el enfoque adecuado de las indagaciones. En otros casos, la *notitia criminis* procede de ciudadanos, colectivos y/o entidades diversas que representan los intereses de uno o más perjudicados por actividades ilícitas *online* y que optan por dirigirse directamente a la Fiscalía. No faltan tampoco las denuncias remitidas por instituciones y organismos de carácter público a las que también han de sumarse aquellos otros supuestos en los que la apertura de diligencias se realiza de oficio por la propia Fiscalía al tener conocimiento, por cualquier otro medio, de hechos que pudieran ser constitutivos de delito.

El detalle de las diligencias incoadas en atención a la conducta investigada es el siguiente:

Delitos informáticos		Diligencias de investigación	%
Contra la libertad	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss.)	4	1,99
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189)	8	3,98
	Acosos menores a través de TICs (art. 183 ter)	3	1,49
	Otros delitos c/libertad sexual a través TIC	8	3,98

Delitos informáticos		Diligencias de investigación	%
Contra la intimidad	Ataques / interceptación sistemas y datos (art. 197 bis y ter)	3	1,49
	Descubrimiento/ revelación secretos a través TIC (art. 197)	16	7,96
Contra el honor	Calumnias/ injurias autoridades a través TIC (arts. 215 y ss.)	10	4,98
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (arts. 248 y 249)	106	52,74
	Descubrimiento secretos empresa a través de TIC (arts. 278 y ss.)	2	1,00
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286)	1	0,50
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	4	1,99
	Delitos c/ propiedad intelectual a través TIC (arts. 270 y ss.)	3	1,49
De falsedad	Falsificación a través de las TICs	2	1,00
Contra Constitución	Discriminación a través TIC (art. 510)	31	15,42
Total		201	100,00

En el año 2019 se incoaron por las fiscalías territoriales 199 diligencias de investigación penal y otras 36 por la propia Unidad Especializada de la Fiscalía General del Estado. No obstante, en relación con estas últimas, ha de aclarase que 34 de ellas tuvieron únicamente por objeto, tal y como contempla la Circular 4/2013 de la FGE, la práctica de las diligencias imprescindibles para la determinación del órgano del Ministerio Fiscal competente para asumir la investigación, razón por la cual, una vez concretado dicho extremo, fueron remitidas a la fiscalía correspondiente para su ulterior tramitación. Las dos restantes, únicas computadas a efectos estadísticos en la tabla adjunta, fueron tramitadas íntegramente en la Unidad Especializada al haberse asignado la investigación a la Fiscal de Sala Coordinadora por Decreto de la Excma. Sra. Fiscal General del Estado, al amparo de lo establecido en el artículo 20.1.º a) y 3.º del Estatuto Orgánico, en atención a la naturaleza y gravedad de los hechos objeto de indagación. En ambos casos, la investigación tuvo por objeto presuntos ataques informáticos a altas instituciones del Estado y las diligencias practicadas en la Fiscalía dieron lugar finalmente a la presentación de denuncia ante los juzgados de instrucción de Madrid, hallándose en la actualidad en tramitación los respectivos procedimientos judiciales.

Como puede observarse, el volumen más significativo de diligencias de investigación corresponde a las que tuvieron por objeto conductas de estafa/defraudación que sumaron 106, en lógica correspondencia al importante volumen de denuncias por este tipo de ilícitos al que hemos hecho referencia varias veces en esta memoria. Le siguen en importancia las 31 relativas a delitos de odio y discriminación cometidas a través de la red y las dedicadas a la investigación de delitos de descubrimiento y revelación de secretos que ascendieron a 16.