

8.2 **Análisis de las diligencias de investigación y procedimientos judiciales incoados y acusaciones formuladas por el Ministerio Fiscal en 2023**

Este apartado de la Memoria anual es el que reviste un mayor interés pues es donde dejamos constancia de nuestra percepción acerca de la evolución de un fenómeno criminal que, por planificarse y ejecutarse –al menos parcialmente– en el ciberespacio y servirse de unos mecanismos e instrumentos digitales en constante desarrollo, ofrece cada día novedades y situaciones emergentes que obligan a investigadores y juristas a buscar nuevas formas de averiguación de los hechos y sus responsables, a reflexionar o repensar la interpretación o forma de aplicación de las normas legales o, incluso, a sugerir al legislador la definición o adecuación de los tipos penales o de los medios de investigación criminal a esas inéditas circunstancias.

Nuestra pretensión, por tanto, es poner a disposición de los poderes públicos y de los ciudadanos, tal y como preceptúa el art. 9 del Estatuto Orgánico, el resultado del trabajo serio y profesional realizado durante el año frente a los ilícitos *online* por un gran equipo de más de 160 fiscales, desplegados por todo el territorio nacional, con el valioso e inestimable apoyo de las unidades policiales especializadas en esta materia y de los órganos judiciales.

Esta común experiencia nos permite también reflexionar sobre las causas de este fenómeno, su incidencia en las distintas manifestaciones criminales, las nuevas formas de comisión –ya detectadas o que pueden generarse en el futuro al hilo de imparable avances técnicos, como los derivados de la IA–, los efectos que todo ello está produciendo en la ciudadanía e igualmente sobre las dificultades que estamos encontrando en la investigación y persecución de estas conductas, y los medios y herramientas más adecuadas para combatirlas. Se trata de promover y facilitar la toma de decisiones, ya sean legislativas, estructurales u organizativas, acerca de las medidas más convenientes para mejorar la eficacia del Estado de Derecho ante esta forma de delincuencia.

Con dicho objetivo, en este apartado de la Memoria reseñamos y analizamos los datos estadísticos registrados por la Institución en el año 2023 acerca de investigaciones, tanto judiciales como del MF, iniciadas en dicho periodo y también sobre los escritos de acusación de la especialidad por actividades delictivas que, en atención a su naturaleza o bienes jurídicos afectados o porque su ejecución se ha llevado a efecto en el entorno virtual, son susceptibles de encuadrarse en el concepto de ciberdelincuencia que se define en la Instrucción 2/2011 de

la Fiscalía General del Estado sobre *el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscaías*.

Es importante dejar constancia de que los datos con los que contamos provienen de la información facilitada por los distintos órganos territoriales de la Institución, obtenida por los fiscales con ocasión de la tramitación de diligencias de investigación, o de nuestras intervenciones procesales en expedientes de los órganos judiciales y en actos de juicio oral, así como del seguimiento de las múltiples operaciones e investigaciones llevadas a efecto durante el año por los cuerpos policiales nacionales y autonómicos relativas a actividades criminales de esta naturaleza. A results de esa información, reflejada en el cuadro incorporado a continuación, en el año 2023 se registraron en España un total de 23.486 procedimientos judiciales y 498 diligencias de investigación penal del Ministerio Fiscal por delitos competencia de esta área de especialización. Dicha cifra supone un descenso en un 4,61% respecto del año 2022 en lo que atañe al volumen de procedimientos judiciales incoados y un incremento de más de un 100% en el de diligencias de investigación penal.

Este descenso en el número de causas judiciales registradas por la Fiscalía —el primero que se detecta desde el año 2016— en ningún caso puede ser interpretado como el reflejo de una tendencia a la baja o de una disminución en la incidencia de la actividad delictiva en el entorno virtual. Por el contrario, los datos que ofrece el Ministerio del Interior en el Balance sobre Criminalidad del año 2023 dan cuenta de una realidad muy diferente, que se concreta en un índice de crecimiento del 25,5% en el conjunto de investigaciones de todos los cuerpos policiales en materia de cibercriminalidad en el periodo interanual 2022-2023, ligeramente superior en lo que se refiere a las estafas y defraudaciones donde el repunte alcanza el 27%.

Varias son las razones que explican la evidente discordancia en los resultados que estamos comentando. En primer término, ha de recordarse que a tenor de lo dispuesto en el art. 284 LECrim, un número muy considerable de las investigaciones iniciadas por los cuerpos policiales no son remitidas a los órganos judiciales ni a la Fiscalía ya que, salvo en algunos supuestos excepcionales, dicho traslado solo es obligado cuando ha sido identificado el autor del hecho ilícito o existen vías de investigación que permiten su averiguación mediante la práctica de las diligencias oportunas, por lo que los datos que se recogen en las estadísticas judiciales o del Ministerio Fiscal en ningún caso van a coincidir con los datos estadísticos policiales.

Pero concurre también una segunda circunstancia que determina que nuestras estadísticas no ofrezcan garantías suficientes de exactitud a efectos de acreditar ni el volumen de expedientes judiciales y/o del Ministerio Fiscal que se incoan anualmente ni, por ende, el porcentaje de ilícitos de una u otra naturaleza que son objeto de los mismos. Nos referimos a las carencias de las aplicaciones informáticas en las que se registran las denuncias, atestados o actuaciones de cualquier tipo relativas a presuntos ciberdelitos que llegan a conocimiento de los órganos de la jurisdicción penal. La falta de previsión específica de una buena parte de los tipos penales de esta naturaleza en los catálogos de infracciones que incorporan dichas aplicaciones es especialmente significativa en aquellos casos, como las estafas y defraudaciones, en los que el mismo *nomen iuris* acoge delitos tradicionales y otros de carácter esencialmente tecnológico. Esta coyuntura, desde hace años, viene obligando a las/os fiscales delegadas/os territoriales de la especialidad a hacer un seguimiento individualizado de todos estos expedientes, para asegurar la corrección de su anotación inicial o, en su caso, su rectificación posterior, de forma que quede adecuadamente reseñada en el registro informático la naturaleza ciber del ilícito de que se trate, labor que resulta muy compleja en aquellos órganos territoriales en los que la información de que disponen las fiscalías procede de la migración de los datos grabados en las oficinas judiciales para las que la calificación jurídica del hecho, como delito de uno u otro tipo, carece de interés en esta fase inicial de la tramitación procesal.

Estas carencias, solventadas año a año por los miembros de la red de especialistas a partir de un esfuerzo personal digno de reconocimiento, se han ido complicando a medida que ha ido aumentando la actividad ilícita en la red, pues dicha progresión dificulta cada vez más ese seguimiento individualizado y casi artesanal de todos los expedientes que se incoan anualmente por este tipo de delitos. Es decir, cuanto más crece la ciberdelincuencia más necesario se hace contar con sistemas de registro debidamente desarrollados, que permitan anotar/consultar con facilidad y separadamente no solo las múltiples figuras típicas incluidas en cada una de las categorías delictivas sino también las distintas variantes de las acciones susceptibles de encuadrarse en cada uno de los tipos penales y, por ello, las limitaciones existentes para lograr ese objetivo resultan más evidentes cada anualidad.

Queremos dejar constancia de estos extremos no solo para justificar la insuficiencia y las carencias en los datos que ofrecemos sino, también, para llamar la atención sobre el extraordinario valor de las

conclusiones que pudieran obtenerse si la información disponible estuviera avalada por un control más detallado y preciso de los expedientes relacionados con esta peligrosa actividad criminal. A modo de ejemplo, y en referencia a una de las materias que está generando una mayor preocupación social, sería de especial interés disponer de un cómputo disgregado de los procedimientos relativos a las diferentes conductas relativas a material de abuso sexual infantil –elaboración, distribución o posesión–, así como de la evolución de cada una de ellas, a efectos de lograr un conocimiento mejor y más completo de las causas y circunstancias que están influyendo en el incremento de estos ilícitos. De esta forma estaríamos en mejores condiciones de vislumbrar las medidas legales u operativas más adecuadas para abordar con mayor rigor y eficacia este grave y peligroso fenómeno criminal. Y lo mismo podríamos decir de las distintas formas de ataque a sistemas informáticos –*ransomware*; *Ddos*; *malware*, etc.– que genéricamente catalogamos como daños informáticos o de las múltiples formas de defraudación –estafas tradicionales *online*; fraude informático; uso irregular de instrumentos de pago o actos preparatorios– que se registran bajo la denominación común de delitos de estafa.

Sin perjuicio de lo anteriormente referido, la obligada intervención del Ministerio Fiscal en la casi totalidad de procedimientos por delitos que se tramitan por los órganos judiciales del Estado y nuestra capacidad de coordinación interna, en atención a los principios que inspiran nuestra actuación, nos colocan en una situación privilegiada para realizar la función a la que antes nos referíamos y que justifica la propia elaboración de esta Memoria, a saber, analizar la información derivada de investigaciones por ciberdelitos y reflexionar acerca de su evolución, variaciones y consecuencias que generan en los derechos de los ciudadanos y el interés general e incluso, como indica el Estatuto Orgánico, efectuar las sugerencias oportunas acerca de *la prevención del delito y las reformas convenientes para una mayor eficacia de la Justicia*.

Como hemos indicado, los procedimientos judiciales registrados por la Fiscalía en 2023 ascendieron a 23.486, cuya distribución por tipología delictiva es la siguiente:

Delitos informáticos		Procedimientos judiciales incoados	%
Contra la libertad	Amenazas/coacciones a través de TIC (art 169 y ss y 172 y ss)	1242	5,29
	Acoso a través de TIC (art 172 ter)	403	1,72

Delitos informáticos		Procedimientos judiciales incoados	%
Contra la integridad moral	Trato degradante a través de TIC (art 173)	63	0,27
Contra la libertad sexual	Pornografía infantil/discapaces a través de TIC (art 189)	610	2,60
	Acoso menores a través de TIC (art 183 ter)	184	0,78
	Otros delitos c/libertad sexual a través TIC	348	1,48
Contra la intimidad	Ataques/interceptación sistemas y datos (art 197 bis y ter)	94	0,40
	Difusión in consentida de imágenes íntimas (art 197.7)	97	0,41
	Descubrimiento/ revelación secretos a través TIC (art 197)	395	1,68
Contra el honor	Calumnias/injurias autoridades a través TIC (art 215)	61	0,26
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TIC (art 248 y 249)	19.464	82,87
	Descubrimiento secretos empresa a través TIC (art 278 y ss)	53	0,23
	Delitos c/ servicios de radiodifusión/interactivos (art 286)	7	0,03
	Delitos de daños informáticos (art 264, 264 bis y 264 ter)	130	0,55
	Delitos c/ propiedad intelectual a través TIC (art 20 y ss)	49	0,21
De falsedad	Falsificación a través de las TIC	114	0,49
Contra Constitución	Discriminación a través de TIC (art 510)	60	0,26
Otros		112	0,48
Total.		23.486	100,00

8.2.1 PROCEDIMIENTOS POR DELITOS DE ESTAFA O DEFRAUDACIÓN

Al igual que en años precedentes, la cifra más elevada corresponde a los procedimientos judiciales por estafas y defraudaciones que ascienden a 19.464, lo que supone un 82,87% del total de los incoados en el año por delitos competencia de esta área de especialización. Este elevadísimo índice confirma la total preeminencia de las investigaciones por esta categoría de ilícitos que además se va incrementando año

a año. Así, es significativo que este indicador, que en 2020 fue de 72,43%, se elevara al 75,50% en 2021 y al 81,68% en el año 2022, para alcanzar el 83,14% en el año memorial y ello pese a que, por las razones antes indicadas, las cifras absolutas obtenidas por este concepto el pasado año –19.449– son ligeramente inferiores a las 20.111 de la anualidad precedente. Asimismo, los datos que ofrece el Ministerio del Interior en el Informe sobre Cibercriminalidad relativo a 2023 reflejan una misma realidad que, como ya hemos indicado, se concreta en un incremento del 27% de las investigaciones policiales por estafa o defraudación que, en dicho periodo, alcanzaron el 90,7% de las iniciadas por cualquier clase de ciberdelitos. A mayor abundamiento, del análisis comparativo de la información plasmada en el citado documento, se colige que el número de diligencias por estafas cometidas *online* se ha incrementado en un 508,1% entre el año 2016 y el pasado 2023.

No obstante, a efectos de dimensionar adecuadamente estos datos y, por ende, la incidencia efectiva de esta tipología criminal en el conjunto de las actividades ilícitas que se planifican y ejecutan en el entorno virtual, es necesario efectuar algunas precisiones. Así, en primer término, ha de recordarse que las estafas y defraudaciones son conductas delictivas que por su naturaleza suelen ser objeto de denuncia por parte de las/os perjudicadas/os con más facilidad que otra clase de conductas que no afloran con habitualidad –tales como los delitos contra la libertad sexual de las/os menores o las vulneraciones de datos o sistemas informáticos– lo que indudablemente influye en los datos estadísticos que analizamos. Como también tiene clara influencia, a esos efectos, la circunstancia, propia de la desvinculación geográfica de las acciones *online*, de que las múltiples víctimas de una misma actividad delictiva puedan presentar denuncia por el perjuicio causado ante cuerpos policiales u órganos judiciales distintos y en diferentes territorios, dando lugar con ello a la incoación de una pluralidad de investigaciones policiales o judiciales que, a su vez, darán lugar a diversas anotaciones estadísticas independientes entre sí. Ciertamente, el desarrollo de la investigación podrá determinar la acumulación de todas ellas en un solo procedimiento si se acredita su efectiva vinculación, aunque a efectos estadísticos, la inicial anotación registral de cada una de las denuncias resulta prácticamente irreversible.

Pero además ha de tenerse en cuenta que, a su vez, la categoría correspondiente a las estafas y defraudaciones abarca una gran diversidad de conductas delictivas que obedecen a dinámicas criminales muy diferentes aun cuando tengan como elemento común el desplazamiento patrimonial irregular en perjuicio de una o más personas y en

beneficio del delincuente o de un tercero. El análisis de los vigentes artículos 248 y 249 CP, en su redacción dada por la Ley Orgánica 14/2022, de 22 de diciembre, deja clara constancia de ello. Dentro de esta categoría computamos no solo las estafas tradicionales, basadas en el engaño, cuando presentan determinadas connotaciones y se cometen *online*, sino también los fraudes propiamente informáticos, así como el uso irregular de instrumentos de pago distintos del efectivo materiales o inmateriales y las diversas conductas que sancionan los actos preparatorios de unos y otras. Ello, en cierta medida, justifica también el elevado volumen de investigaciones que se incoan anualmente por estos delitos.

En cualquier caso, y con las indicadas matizaciones, la relevancia de estas actividades delictivas es incuestionable, como lo son también los perjuicios que anualmente causan a las/os ciudadanas/os, empresas e incluso a los Estados. Según resulta de la encuesta sobre *inseguridad en la red* elaborada por el CIS en febrero de este mismo año, el 47,5% de los/as entrevistados había sido víctima de estafa o de intento de estafa en el último año y, efectivamente, ha de reconocerse que las posibilidades de llevar a efecto acciones de esta naturaleza en perjuicio de otro se han visto amplificadas por las capacidades de acción que el desarrollo tecnológico ha puesto a disposición de los/as usuarios de la red.

Así, es incuestionable que el nivel de conectividad interpersonal que proporcionan estas tecnologías está facilitando la difusión del engaño como vector esencial en torno al cual se articula la estafa tradicional. Son numerosas y muy variadas las actividades ilícitas que se sustentan en esta dinámica criminal y en las que los/as delinquentes se sirven de los diferentes medios de comunicación *online*, tales como foros, chats o sitios web, para captar mediante técnicas de ingeniería social a sus víctimas, al tiempo que recurren a diversos instrumentos y argucias para ocultar su identidad y asegurarse la impunidad. Entre ellas pueden mencionarse, a modo de ejemplo, las ofertas fraudulentas de todo tipo de bienes y servicios; las propuestas falsas de empleo que requieren de la víctima la entrega de cierta cantidad de dinero; la utilización fraudulenta de la plataforma *bizum*; la estafa del amor –*romance scam*–; las cartas nigerianas; así como los diferentes supuestos en que el delincuente, a través de mecanismos como el *smishing* o el *vishing*, simula actuar en nombre de entidades bancarias o de cualquier clase de empresa o institución o también cuando usurpa con fines fraudulentos la identidad de otra persona, como es el caso de la *estafa del hijo en apuros*, en la que el estafador se hace pasar por un familiar cercano de la víctima demandándole la entrega de una cantidad de

dinero por encontrarse supuestamente en situación de urgencia. Algunos de estos supuestos, particularmente aquellos en que se utiliza la identidad de alguien realmente existente, se están viendo extraordinariamente favorecidos por el uso de la inteligencia artificial lo que, en nuestra opinión, hace más necesaria que nunca la tipificación específica de estas conductas de simulación *online* de identidad ajena a fin de contar con una herramienta legal que permita una actuación más directa y efectiva frente a este tipo de comportamientos, cualquiera que sea la finalidad que con ello se pretenda.

Como ya hemos indicado en años precedentes, la frecuencia con que detectamos el uso en el entorno virtual de la identidad de otra persona para defraudar o para efectuar irregularmente todo tipo de actividades económicas, tales como solicitud de préstamos, compraventas, contratación de servicios, apertura de cuentas corrientes etc., está creciendo de forma muy alarmante, afectando a un número cada vez mayor de ciudadanos y ciudadanas que se ven implicados en procedimientos judiciales o que son objeto de reclamaciones económicas por actividades en las que no han intervenido. Desde nuestro punto de vista, son varias las líneas de actuación en las que habría que trabajar para evitar o reducir al máximo estas situaciones y proteger los intereses de los/as afectados. Así, en primer término, parece imprescindible establecer un sistema adecuado de registro y tratamiento de la información policial relativa a esta clase de actividades ilícitas que permita relacionar entre sí unos y otros hechos y, en consecuencia, detectar tempranamente la usurpación. Pero también sería de extraordinario interés reforzar las medidas de seguridad en las operaciones de la banca *online* para prevenir este tipo de situaciones, ya que la habitualidad con la que una buena parte de las/os ciudadanas/os recurre a este tipo de servicios exige, a nuestro modo de ver, la instauración de controles más efectivos de la identidad real de quienes intervienen en dichas operaciones.

Las defraudaciones cometidas mediante ofertas maliciosas de inversiones aparentemente seguras, ventajosas y con buenas perspectivas de obtener sustanciosos beneficios económicos son también frecuentes en la red. Articuladas esencialmente en el engaño a la víctima, en muchas ocasiones se publicitan a través de plataformas muy sofisticadas y técnicamente preparadas para generar la confianza de las/os usuarias/os de internet y determinarles a realizar disposiciones económicas, ya sea en moneda de curso legal, valor monetario o criptomoneda, que el delincuente o delincuentes hacen suyas en propio beneficio y en perjuicio del inversor/a.

Estas modalidades de fraude proliferan en el ciberespacio aprovechando el auge del comercio electrónico y la economía digital y frecuentemente están organizadas y/o dirigidas por grupos criminales de dimensión transnacional. La complejidad que entraña el esclarecimiento de estas actividades criminales, como consecuencia de la agilidad de las operaciones interbancarias y la utilización frecuente por los delincuentes de entidades financieras radicadas en el extranjero, se agrava considerablemente cuando la defraudación se realiza en monedas virtuales dada las dificultades que entraña la *blockchain* para la trazabilidad de los movimientos económicos y la identificación de las/os intervinientes en los mismos. Por ello han sido bienvenidos los recientes desarrollos normativos nacionales e internacionales en esta materia que, entre otros avances, han traído consigo la puesta en funcionamiento de un registro de proveedores de servicios de intercambio de moneda y custodia de *wallets*, así como la mejora de herramientas legales de cooperación internacional.

No obstante, la incidencia progresiva de las defraudaciones que se sirven de criptovalores para el desarrollo del *iter criminis* demanda algunas soluciones adicionales que faciliten la actuación de los investigadores y de los órganos de la jurisdicción penal, entre ellas resulta ya imprescindible la elaboración de un protocolo de actuación, con intervención de la ORGA, para articular adecuadamente las gestiones relacionadas con el almacenamiento y, en su caso, realización de las criptomonedas incautadas con ocasión de investigaciones criminales.

Como se colige de los anteriores comentarios, en múltiples ocasiones las/os delincuentes combinan hábilmente el engaño con la manipulación de datos y sistemas informáticos para lograr sus propósitos. La limitada extensión de estas reflexiones nos impide explayarnos en este punto concreto, pero ha de reseñarse que una buena parte de las/os fiscales delegados, dan cuenta de procedimientos por actividades delictivas como el *SIM Swapping* –basado en la sustitución de la tarjeta SIM de los terminales telefónicos para burlar los sistemas de seguridad de la banca *online*– los ataques Business Email Compromise (BEC) –también conocidos como fraude del CEO y dirigidos generalmente contra entidades empresariales– o el robo de credenciales y datos personales mediante accesos irregulares a dispositivos o sistemas de almacenamiento para su posterior utilización con fines fraudulentos. Todas ellas son dinámicas criminales muy versátiles que las/os delincuentes adaptan fácilmente a las circunstancias personales de sus víctimas y a los propósitos ilícitos que pretenden y que año a año generan cada vez más perjuicios económicos.

Finalmente son de obligada referencia en este apartado las acciones ilícitas relacionadas con instrumentos de pago distintos del efectivo. La implementación por el legislador español de la Directiva (UE) 2019/713 sobre fraude y falsificación de medios de pago distintos del efectivo, se ha materializado con la inclusión de los instrumentos de pago de carácter inmaterial como objeto de protección penal y la tipificación en el art. 249.2 CP de los actos preparatorios de dichas conductas, medidas que esperamos contribuyan a abordar más eficazmente estos ilícitos. Resulta necesario que así sea ya que, al tratarse de comportamientos en los que el desplazamiento patrimonial irregular se articula a partir de medios de pago susceptibles de utilizarse *online* en cualquier lugar del mundo, constituyen una de las actividades criminales que actualmente presenta mayores dificultades en su esclarecimiento, persecución y sanción y, por ello también para el resarcimiento del perjuicio causado, ya sea a las propias víctimas o a las entidades bancarias, cuya obligación de cubrir los daños generados parece insoslayable, particularmente si no se han adoptado por su parte las medidas de seguridad necesarias para evitarlo.

La interpretación y aplicación de estos tipos penales plantea, no obstante, cuestiones jurídicas de interés que ya están siendo analizadas por la Institución a efectos de fijar criterios comunes de actuación. Sirva como ejemplo de ello las Conclusiones adoptadas en las Jornadas de Fiscales especialistas en cibercrimen, celebradas en diciembre del pasado 2023 o la reciente publicación de la Consulta 1/2024 de la FGE sobre algunas cuestiones relacionadas con la utilización fraudulenta de instrumentos de pago distintos del efectivo.

8.2.2 PROCEDIMIENTOS POR DELITOS CONTRA BIENES PERSONALÍSIMOS

Aunque con un porcentaje muy inferior, las agresiones contra bienes personalísimos son, sin duda, una de las manifestaciones criminales de mayor interés y trascendencia de entre las que se planifican en el ciberespacio. En este apartado incluimos los ataques contra la libertad y seguridad de las personas, contra su integridad moral, su libertad sexual, su honor y los que afectan a la intimidad en el entorno virtual.

Según la información disponible, las causas judiciales iniciadas por estos ilícitos alcanzaron el pasado año la cifra de 3.403, lo que supone un 14,43% del total de las incoaciones por cibercrimitos, entre las que destacan especialmente las correspondientes a ilícitos contra la libertad y seguridad que generaron 1.645 anotaciones y las relacio-

nadas específicamente con ataques a la libertad sexual que sumaron 1.142.

Entre las primeros, el índice más elevado corresponde a las amenazas y coacciones cometidas a través de las TIC que motivaron 1.242 incoaciones en los órganos judiciales, cifra muy similar a la del año precedente –1.248– circunstancia ya de por sí reveladora del crecimiento efectivo de las investigaciones por hechos de esta naturaleza pues, pese al comentado descenso en el cómputo total de procedimientos por ciberdelitos, su volumen se mantiene constante. No ocurre lo mismo con las causas sobre acoso permanente u hostigamiento, que sumaron en conjunto 403, cifra inferior en un 14% a la del año 2022 si bien condicionada por el descenso generalizado en los datos estadísticos que venimos comentando. En cualquier caso, ha de tenerse en cuenta que muchas de las anotaciones por hechos de este tipo, aunque se cometan a través de la red, escapan al control numérico de esta área de especialización al afectar de lleno al área de violencia contra la mujer, en la que son objeto de un tratamiento más específico.

Los procedimientos contra la integridad moral de las víctimas, aun cuando únicamente suponen el 0,27% del total de expedientes iniciados, merecen en esta ocasión una mención específica ya que es precisamente en esta figura del art 173 CP en la que estamos incardinando las conductas, todavía novedosas pero que ya han sido objeto de investigación e incluso de algún escrito de acusación, en las que las/os delinquentes se sirven de sistemas de inteligencia artificial para elaborar contenidos pornográficos a partir de imágenes reales de personas adultas –en ocasiones previamente sustraídas u obtenidas en cualquier otra forma irregular– y publicitarlas posteriormente a través de la red. Dada la naturaleza de las imágenes así elaboradas y difundidas, la sanción de estas conductas con base en dicho precepto resulta por el momento suficiente. No obstante, sería oportuno plantearse una tipificación penal más específica que diera cobertura a aquellos otros supuestos en los que, por las características del contenido elaborado y/o difundido, no se vea afectada la integridad moral de la víctima sino otros bienes jurídicos como, por ejemplo, la intimidad personal.

Consideración independiente merecen, sin duda, los procedimientos incoados por delitos contra la libertad sexual que en conjunto dieron lugar a 1.142 incoaciones que suponen casi el 5% del total de los registrados en el año por ciberdelitos. Dicha cifra, aun siendo notablemente inferior a la de 2022, en ningún caso puede atribuirse a una efectiva disminución en la comisión de este tipo de actividades delictivas, sino a las disfunciones en el registro de expedientes a que hemos hecho referencia anteriormente. Como se señala en el apartado de esta Memoria

dedicado a los menores y las redes sociales, los ilícitos que atentan contra la libertad sexual de los menores, tanto los relativos a material de abuso sexual infantil (CSAM) como a otras formas más graves de agresión *online*, se han ido incrementando en los últimos años –tal y como se colige de indicadores nacionales e internacionales debidamente acreditados– no solo en el aspecto meramente cuantitativo sino también en cuanto al alcance y circunstancias en que se produce la agresión, los efectos lesivos generados y, por supuesto, en el número de víctimas ya que, lamentablemente, en la mayoría de las investigaciones de este tipo se cuentan por decenas los menores afectados por la ilícita actividad de un único agresor. En ello está incidiendo de forma significativa el uso frecuente y generalizado de las herramientas tecnológicas por parte de un colectivo que, por su edad y grado de desarrollo personal, no se encuentra en condiciones de prever los riesgos derivados de mantener determinados contactos en la red. El problema además se agudiza con la puesta a disposición de los/as ciudadanos/as de sistemas de inteligencia artificial susceptibles de utilizarse para la comisión de algunos de estos ilícitos, especialmente los relacionados con la elaboración y distribución de CSAM, supuestos que ya han determinado la presentación de algunos escritos de acusación por las fiscalías.

Por otra parte, las dificultades para la persecución y sanción de estos gravísimos comportamientos se han ido incrementando como consecuencia del empleo de medios y sistemas de planificación y ejecución cada vez más sofisticados y seguros, tales como los mecanismos de encriptación o los archivos compartidos en la nube, que complican progresivamente su investigación. Son estas circunstancias las que han determinado la propuesta de la Comisión Europea de reformar la Directiva (UE) 2011/93 sobre abuso, explotación sexual de los menores y pornografía infantil, modificación con la que se pretende incluir nuevas herramientas legales para mejorar la respuesta penal frente a estos ilícitos, y también las que han dado lugar en nuestro país al inicio de los trabajos para la elaboración de un ley integral de protección de los menores en el entorno virtual que esperamos incorpore modificaciones de interés en esta materia tanto de carácter preventivo como represivo.

Por su parte, los delitos contra la intimidad personal, sancionados en el art 197 C.P, determinaron en 2023 la incoación de 492 procedimientos a los que han de sumarse los 94 que tuvieron por objeto investigar accesos o interceptaciones irregulares en sistemas informáticos con la finalidad de atentar contra ese mismo bien jurídico. La cifra total, que asciende a 586, es superior en casi un 12% a la obtenida por esta categoría en el año 2022, lo que da cuenta del incremento de estas

acciones delictivas entre las que deben mencionarse, como especialmente graves por sus consecuencias en los derechos de los ciudadanos, los ataques planificados y ejecutados por grupos de delincuencia organizada contra grandes entidades de carácter público o privado para apoderarse de información personal almacenada en sus sistemas de los que son buen ejemplo los dirigidos contra el Hospital Clinic de Barcelona o la entidad Air Europa.

8.2.3 PROCEDIMIENTOS POR DELITOS DE DAÑOS INFORMÁTICOS

Muy relacionados con estos últimos, han de citarse también los 130 expedientes relativos a daños en datos o sistemas (arts. 264 y ss. CP), cifra muy similar a la registrada en 2022 por este mismo concepto, pese al descenso en el cómputo general de expedientes registrados. Este resultado confirma la incidencia creciente de estas agresiones, pero también da cuenta de la efectividad de los mecanismos administrativos establecidos para garantizar la notificación de incidentes de seguridad a los Equipos de respuesta inmediata a incidentes de seguridad (CSIRTs) correspondientes y el posterior traslado de esa información, a través de la Oficina de Coordinación de Ciberseguridad (OCC), a los cuerpos policiales y al MF cuando se detecten indicios de actividad delictiva, a los efectos de su ulterior seguimiento y judicialización si procediere. Buena muestra de ello son las múltiples investigaciones tramitadas por los órganos judiciales por agresiones de esta naturaleza, entre las que destacan por su frecuencia y gravedad los ataques de *ransomware* en sus diversas variantes que pueden derivar en la exfiltración de datos y ulterior amenaza de su difusión a través de la red o también, entre otros, los ataques DDoS que ocasionalmente se plantean como acciones de protesta o de reacción frente a relevantes acontecimientos políticos lo que podría llevar a vincularlos con actividades de desinformación o amenazas híbridas.

8.2.4 ESCRITOS DE ACUSACIÓN

La información sobre escritos de acusación presentados por el Ministerio Fiscal tiene, sin duda, un relevante interés en el estudio que abordamos ya que da cuenta de aquellos supuestos en los que los fiscales, culminado el proceso de investigación, estiman procedente acusar a persona o personas concretas por considerarla/s responsables de hechos perfectamente definidos y encuadrables en alguno de los ilícitos

tos que sanciona nuestro código penal. Se trata por tanto de una información generada por la propia Institución y que deriva del estudio serio y reflexivo, tanto fáctico como jurídico, de los procedimientos en los que se formula y que, por ello, resulta muy valiosa para el análisis de la incidencia de la ciberdelincuencia en sus diversas manifestaciones y de nuestra respuesta frente a estos ilícitos.

Según los datos remitidos por los órganos territoriales, en el año 2023 el Ministerio Fiscal formuló 3.583 escritos de acusación por delitos competencia del área de especialización cuyo detalle es el siguiente:

Delitos informáticos		Calificaciones	%
Contra la libertad	Amenazas/coacciones a través de TIC (art 169 y ss y 172 y ss)	344	9,60
	Acoso a través de TIC (art 172 ter)	140	3,91
Contra la integridad moral	Trato degradante a través de TIC (art 173)	55	1,54
Contra la libertad sexual	Pornografía infantil/discapaces a través de TIC (art 189)	348	9,71
	Acoso menores a través de TIC (art 183 ter)	71	1,98
	Otros delitos c/libertad sexual a través TIC	125	3,49
Contra la intimidad	Ataques/interceptación sistemas y datos (art 197 bis y ter)	16	0,45
	Difusión in consentida de imágenes íntimas (art 197.7)	38	1,06
	Descubrimiento/ revelación secretos a través TIC (art 197)	131	3,66
Contra el honor	Calumnias/injurias autoridades a través TIC (art 215)	11	0,31
Contra el patrimonio y el orden socioeconómico	Estafa cometida a través de las TIC (art 248 y 249)	2.172	60,62
	Descubrimiento secretos empresa a través TIC (art 278 y ss)	12	0,33
	Delitos c/ servicios de radiodifusión/interactivos (art 286)	5	0,14
	Delitos de daños informáticos (art 264, 264 bis y 264 ter)	17	0,47
	Delitos c/ propiedad intelectual a través TIC (art 20 y ss)	11	0,31
De falsedad	Falsificación a través de las TIC	69	1,93
Contra Constitución	Discriminación a través de TIC (art 510)	15	0,42

Delitos informáticos		Calificaciones	%
Otros		3	0,08
Total		3.583	100,00

Como es habitual, el volumen más elevado corresponde a las acusaciones por delitos de estafa y defraudación, que ascendieron a 2.172, más de un 60% del total de las formuladas durante el año. La falta de precisión en las tablas estadísticas, a la que anteriormente hacíamos referencia, impide detallar, como sería deseable, la conducta delictiva concreta a que se refiere cada una de las anotaciones, pero, a partir de nuestra experiencia, podemos afirmar que las más habituales son las relativas a actividades fraudulentas *online* basadas en el engaño o aquellas en las que éste se combina con manipulaciones en datos y sistemas informáticos. Por el contrario, son menos frecuentes las relacionadas con el uso irregular de instrumentos de pago, dada las dificultades que plantea su investigación por las razones ya apuntadas, lo que en demasiadas ocasiones determina la imposibilidad de dirigir la acusación contra persona/s concreta/s.

Le siguen en importancia numérica las acusaciones por delitos relacionados con material de abuso sexual infantil, que sumaron el pasado año 348, un 9,71% del total registrado, a las que han de sumarse las 71 por acoso a menores a través de las TIC y las 125 por otros ilícitos contra la libertad sexual, entre los que se incluyen actuaciones gravísimas como las agresiones sexuales en el entorno virtual –con o sin introducción de objetos– o las acciones de exhibicionismo o provocación sexual, lo que eleva la cifra resultante por esta categoría de delitos a 544, algo más del 15% del total de acusaciones formuladas. Este dato, muy similar en su conjunto y en los distintos conceptos que la componen, al obtenido en la anualidad precedente, refleja una cierta estabilidad en la respuesta penal frente a estas agresiones. A efectos de valorar adecuadamente la información estadística que ofrecemos, es preciso reseñar que, con frecuencia, aunque la acusación se formule contra una única persona, la imputación tiene por objeto una pluralidad de conductas desarrolladas por ésta en espacios temporales prolongados y afectando a un número más o menos elevado de víctimas, de forma tal que en un solo escrito suelen ser objeto de acusación una pluralidad de acciones contra distintas personas. Son además escritos de acusación de especial complejidad en los que concurren una pluralidad de ilícitos distintos tales como *childgrooming*, agresiones sexuales, actos de elaboración y/o distribución de CSAM, gene-

rando cuestiones jurídicas muy complejas sobre las que, en ocasiones, no existen criterios doctrinales o jurisprudenciales asentados.

Los delitos contra la libertad y seguridad dieron también lugar a 484 acusaciones, un 13,5% de las presentadas en el año, de entre las que destacan las relativas a actos *online* de amenaza o de intimidación que fueron 344, cifra ligeramente superior a las 336 del 2022. Las acusaciones por delitos contra bienes personalísimos se completan con las 55 formuladas por delitos contra la integridad moral y las 169 correspondientes a ilícitos contra la intimidad.

En cuanto a los delitos por ataques a datos y sistemas informáticos determinaron la presentación en el año 2023 de un total de 33 escritos de acusación de los que 16 se corresponden con acciones de espionaje informático (art. 197 bis y ter CP) y 17 con actos de sabotaje informático (arts. 264 y ss. CP). En relación con ellos, se detecta un ligero descenso respecto del año 2022 que en cifras absolutas se concreta en 6 escritos de acusación.

8.2.5 DILIGENCIAS DE INVESTIGACIÓN

Este apartado tiene por objeto reflexionar acerca de las investigaciones relativas a ciberdelitos que se tramitan directamente por las fiscalías al amparo de los artículos 5 del EOMF y 773.2.º LECrim. Se trata de actuaciones preprocesales que son iniciadas por la propia Institución ya sea de oficio o en razón, entre otras causas, a denuncias remitidas por organismos o instituciones públicas; deducción de testimonio de procedimientos judiciales; puesta en conocimiento de investigaciones de los Cuerpos y Fuerzas de Seguridad; o denuncias remitidas por entidades de la sociedad civil o por particulares que, al amparo de los artículos 259 y ss. LECrim, trasladan al Ministerio Fiscal información sobre determinados hechos o acontecimientos por entender que presentan indicios de criminalidad.

El alcance y contenido de estas diligencias viene determinado por un doble aspecto: temporal y objetivo. En cuanto al primero porque el art. 5 EOMF establece un plazo máximo de duración de las mismas —6 o 12 meses, según los casos— sin perjuicio de que puedan ser prorrogadas por Decreto del Fiscal General del Estado. Por otra parte, y en atención a su alcance, la capacidad de investigación del Ministerio Fiscal tiene como límite constitucional la práctica de diligencias que exijan autorización judicial, en cuyo caso las actuaciones han de remitirse al órgano judicial competente para la prosecución de la investigación. Precisamente esta última circunstancia tiene una especial

incidencia en la materia que nos ocupa pues buena parte de las investigaciones por ciberdelitos, por su propia naturaleza y porque se planifican y ejecutan con ocasión de procesos de comunicación, precisan la realización de diligencias que, por afectar a derechos fundamentales, exigirán de dicha autorización judicial, lo que condiciona nuestra capacidad de actuación directa en este ámbito.

Pese a estas limitaciones, el volumen de diligencias de investigación incoadas por las fiscalías en el año memorial asciende a 498, cifra que refleja un incremento de más del 100% respecto del año 2022 y, por ende, una dinámica muy activa de los integrantes de la red de especialistas que habitualmente son los encargados de este tipo de actuaciones en los distintos territorios.

El análisis desglosado de estos expedientes es el siguiente:

Delitos informáticos		Diligencias de investigación	%
Contra la libertad	Amenazas/coacciones a través de TIC (art 169 y ss y 172 y ss)	13	2,61
Contra la integridad moral	Acoso a través de TIC (art 172 ter)	9	1,81
	Trato degradante a través de TIC (art 173)	1	0,20
Contra la libertad sexual	Pornografía infantil/discapaces a través de TIC (art 189)	10	2,01
	Acoso menores a través de TIC (art 183 ter)	3	0,60
	Otros delitos c/libertad sexual a través TIC	16	3,21
Contra la intimidad	Ataques/interceptación sistemas y datos (art 197 bis y ter)	4	0,80
	Difusión in consentida de imágenes íntimas (art 197.7)	3	0,60
	Descubrimiento/ revelación secretos a través TIC (art 197)	20	4,02
Contra el honor	Calumnias/injurias autoridades a través TIC (art 215)	10	2,01
Contra el patrimonio y el orden socioeconómico	Estafa cometida a través de las TIC (art 248 y 249)	87	17,47
	Descubrimiento secretos empresa a través TIC (art 278 y ss)	1	0,20
	Delitos de daños informáticos (art 264, 264 bis y 264 ter)	8	1,61
	Delitos c/ propiedad intelectual a través TIC (art 20 y ss)	1	0,20
De falsedad	Falsificación a través de las TIC	1	0,20

Delitos informáticos		Diligencias de investigación	%
Contra Constitución	Discriminación a través de TIC (art 510)	311	62,45
Total.		498	100,00

La primera precisión obligada es la de aclarar que, a diferencia de la información ofrecida en los restantes apartados de esta Memoria que se nutre exclusivamente de datos generados en órganos territoriales, en este apartado se computan también los expedientes de esta naturaleza tramitados por la Unidad Especializada contra la Criminalidad Informática. Efectivamente, del total de diligencias incoadas, un total de 146 corresponden a dicha Unidad especializada de las que 140 tuvieron por objeto ilícitos *online* de odio y/o discriminación. Son supuestos en los que nuestra actuación, de conformidad con lo dispuesto en la Circular 2/2022 FGE, se limita a realizar las averiguaciones imprescindibles para concretar el *forum delicti* comisi y solicitar la preserva de evidencias, trasladando posteriormente las diligencias al Fiscal de Sala Coordinador contra los Delitos de Odio y Discriminación a los efectos de su ulterior tramitación. Con todo, la cifra más elevada se corresponde con las 311 diligencias incoadas por dichos ilícitos, más de un 62% del total, lo que tiene su razón de ser, como se acaba de apuntar, en el elevado número de diligencias incoadas por esta Unidad para la determinación de la competencia territorial y que posteriormente dan lugar a la apertura de diligencias de investigación preprocesal en las diversas fiscalías territoriales competentes.

También es relevante la cifra de las que han sido abiertas para la investigación de estafas o defraudaciones, un 17,47% del total, así como las que tuvieron por objeto ataques contra bienes personalísimos que sumaron un total de 85, poco más del 17% del total, entre las que destacan las 23 iniciadas por delitos contra la intimidad o las 29 por actos contra la libertad sexual en el entorno virtual.

De las 352 diligencias de investigación preprocesal registradas en las fiscalías territoriales, un 16,19% –57 en cifras absolutas– fueron archivadas durante el año y un 45% –161– fueron remitidas a los órganos judiciales para prosecución de la investigación, hallándose las restantes en tramitación en la fecha de elaboración de esta Memoria.