8.2 Análisis de las diligencias de investigación y procedimientos judiciales incoados y acusaciones formuladas por el Ministerio Fiscal en 2024

Una vez más, debemos llamar la atención sobre este apartado de nuestra memoria anual en el que, sobre la base de la experiencia adquirida por los y las fiscales especialistas en la investigación y enjuiciamiento de las distintas manifestaciones de la actividad delictiva en el entorno virtual, reflexionamos acerca de la evolución de este fenómeno criminal en las distintas zonas geográficas y en el conjunto del territorio del Estado, y también sobre las dificultades que hemos detectado en su investigación y persecución penal, tanto en los aspectos de carácter más técnico –relacionados con el esclarecimiento de las acciones ilícitas *online* y la determinación de sus autores– como aquellos otros de naturaleza estrictamente jurídica que se plantean con ocasión de la interpretación y aplicación de los tipos penales a las situaciones fácticas que son sometidas a nuestra consideración.

Esta labor resulta particularmente compleja en una materia tan abierta y versátil como la que nos ocupa y que, como ya se ha indicado, evoluciona constantemente al hilo de los importantes avances técnicos y científicos que los delincuentes no dudan en utilizar para mejorar su capacidad de planificar y ejecutar sus criminales propósitos. Pero, precisamente por ello, son especialmente relevantes estas reflexiones, que realizamos al amparo del artículo 9 de nuestro Estatuto Orgánico, ya que tienen su fundamento y origen en el conocimiento y experiencia derivados de nuestra cotidiana intervención en la investigación y persecución penal de este tipo de conductas. El análisis reflexivo y sosegado de los datos así obtenidos por parte de un equipo integrado por más de 160 profesionales, especialmente cualificados en esta materia, nos permite trasladar a las restantes instituciones, a los poderes públicos y a la ciudadanía, los resultados de este trabajo, así como la información y las valoraciones que estimamos de interés acerca de la forma en que se está planificando la delincuencia en el entorno virtual, de sus manifestaciones más frecuentes o más peligrosas, de sus efectos en la seguridad y en los derechos e intereses de los ciudadanos así como, también, de las carencias o disfunciones que habrían de subsanarse para que la actuación del Estado de Derecho frente a esta forma de delincuencia sea cada vez más eficaz. Con dichas reflexiones tratamos de contribuir a garantizar a la ciudadanía un uso seguro del ciberespacio en las múltiples y variadas actividades en que se concretan las relaciones entre las personas en el entono virtual.

Con ese objetivo iremos desgranando en las siguientes líneas la información de la que disponemos sobre las diversas actividades delictivas que incluimos dentro del concepto de criminalidad informática y que ha sido recopilada por los distintos órganos del Ministerio Fiscal en el curso de las actuaciones desarrolladas por los propios fiscales en los expedientes incoados en el seno de la Institución o con ocasión de nuestra intervención en la coordinación de investigaciones policiales o en las distintas fases de los procesos iniciados y tramitados durante el año 2024 por los órganos judiciales. Lamentablemente, las limitaciones de nuestros sistemas informáticos no nos permiten por el momento ofrecer datos y/o análisis más precisos, pero, aun reconociendo dichas carencias, ha de ponerse en valor el esfuerzo realizado por quienes integran la Red de Especialistas en Criminalidad Informática para hacer posible, en su respectivo ámbito territorial de competencia, no solo una actuación seria y eficaz en las múltiples investigaciones y procesos judiciales seguidos por estos ilícitos, sino también un seguimiento lo más completo y preciso posible de esta peligrosa forma de delincuencia. Los resultados de esta labor son los que tomamos de base para el análisis de situación que ofrecemos a continuación y también para detectar y alertar sobre tendencias y posibles amenazas que debieran ser tenidas en cuenta a efectos del diseño de políticas criminales o de futuras iniciativas de carácter normativo, organizativo o estructural.

Bueno sería, desde nuestro punto de vista, apostar por una mejora efectiva de las aplicaciones de registro informático junto a la adecuada conjunción de aquellas que operan a nivel de todo el Estado con las utilizadas específicamente en las distintas CCAA. La configuración de la Fiscalía como una Institución centralizada, cuya intervención es obligada en la mayoría de los procesos penales por delito, junto con nuestra capacidad de coordinación interna y de trabajo en equipo, coloca a la Institución en una posición única e incuestionablemente privilegiada para el seguimiento y valoración de fenómenos criminales como el que nos ocupa, extraordinariamente versátil, desvinculada de espacios físicos determinados y cuyos efectos pueden manifestarse, simultánea o sucesivamente, en territorios distintos y distantes. No disponer de las herramientas adecuadas para poder gestionar y trabajar adecuadamente la información así obtenida supone a nuestro entender desperdiciar su valor y, por ende, las aportaciones, propuestas y/o sugerencias que de ello pudieran derivarse y que sin duda contribuirían a identificar y focalizar las necesidades más acuciantes, en orden a optimizar nuestra

capacidad de acción frente a la ciberdelincuencia y a minimizar sus perversas y graves consecuencias.

A partir de los datos recopilados por la Institución, respecto de los procedimientos judiciales y diligencias de investigación del Ministerio Fiscal incoados por cualquier clase de conducta delictiva *online* incluida en el ámbito competencial del área de especialización, resulta que en el año 2024 se iniciaron en el conjunto del territorio del Estado 27.104 procedimientos judiciales y 443 diligencias de investigación del Ministerio Fiscal por hechos ilícitos de dicha naturaleza, lo que hace un total de 27.547 expedientes. La comparación de estas cifras con las correspondientes al año 2023, en el que se registraron 23.486 procedimientos judiciales y 498 diligencias de investigación de la Fiscalía, da cuenta de un incremento en conjunto de un 14,86%, que se concreta en un índice del 15,40% en referencia a los procedimientos judiciales y un ligero descenso en el volumen de diligencias de investigación iniciadas por el Ministerio Fiscal.

Estos datos confirman la valoración que efectuábamos en la memoria del pasado año acerca de la leve inflexión detectada en el año 2023, concretada en un 4,61% en el volumen de incoaciones judiciales por ciberdelitos, según la cual ese ligero descenso, que bien puede ser atribuido a problemas de registro estadístico o circunstancias coyunturales, no desvirtúa la tendencia claramente alcista, que venimos detectando en los últimos periodos anuales, de esta forma de delincuencia. De hecho, los índices de crecimiento en el volumen de procedimientos judiciales por delitos de esta naturaleza no pueden ser más expresivos, ya que la cifra obtenida por dicho concepto en el año memorial 27.107– da cuenta de un incremento progresivo, que se concreta en poco más del 10% respecto de los datos correspondientes al año 2022, de casi un 14% en relación con el año 2021 y de un elevadísimo 60,2% en relación con la cifra de 16.914 incoaciones obtenida en el año 2020, anualidad esta última significativamente marcada por la especial situación generada por el COVID–19. Como claramente se deja constancia en la Resolución del Parlamento de la Unión Europea de 10 de junio de 2021, sobre la nueva Estrategia de Ciberseguridad para la Década Digital, la pandemia puso de manifiesto las vulnerabilidades de nuestra sociedad, particularmente en los sectores más críticos, ya que las medidas asociadas al incremento de la conectividad y al teletrabajo, establecidas para paliar los efectos del distanciamiento físico, incrementaron nuestra dependencia de las tecnologías y, entre otras consecuencias, trajeron consigo un aumento significativo, tanto en número como en complejidad, de los ataques informáticos, los ciberdelitos y el uso

malintencionado de las tecnologías en todo el ámbito territorial de la UE. En cualquier caso, y al analizar los datos que ofrecemos, no puede obviarse que estos solo reflejan una parte significativamente reducida del volumen total de denuncias y/o investigaciones policiales por ciberdelitos que en el año 2024, y según datos del Ministerio del Interior, ascendieron a 465.838 ya que, por mor de lo dispuesto en el artículo 284 LECrim, únicamente se trasladan a los órganos de la jurisdicción penal aquellas en las que se ha identificado o puede identificarse a quien puede ser responsable del hecho ilícito. Como tampoco ha de olvidarse el número, imposible de concretar, de conductas delictivas que permanecen ocultas, al no llegar a conocimiento de las autoridades del Estado por alguna de las múltiples razones que iremos analizando a continuación.

El análisis de los datos relativos a los procedimientos judiciales incoados en la pasada anualidad, en atención a las distintas tipologías delictivas, queda reflejado a continuación en los siguientes términos:

Delitos informáticos		Procedimientos judiciales incoados	%
Contra la libertad	Amenazas/coacciones a través de TIC (art. 169 y ss y 172 y ss)	1.528	5,64
	Acoso a través de TIC (art. 172 ter)	318	1,17
Contra la integridad moral	Trato degradante a través de TIC (art. 173)	54	0,20
Contra la libertad sexual	Pornografía infantil/discapacidad a través de TIC (art. 189)	685	2,53
	Acoso menores a través de TIC (art. 183 ter)	186	0,69
	Otros delitos c/libertad sexual a través TIC	326	1,20
Contra la intimidad	Ataques/interceptación sistemas y datos (art. 197 bis y ter)	93	0,34
	Difusión inconsentida de imágenes íntimas (art. 197.7)	107	0,39
	Descubrimiento/revelación secretos a través TIC (art. 197)	443	1,63
Contra el honor	Calumnias/injurias autoridades a través TIC (art. 215)	57	0,21

Delitos informáticos		Procedimientos judiciales incoados	%
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TIC (art. 248 y 249)	22.614	83,43
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss)	23	0,08
	Delitos c/ servicios de radiodifusión/interactivos (art. 286)	82	0,30
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	137	0,51
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss)	82	0,30
De falsedad	Falsificación a través de las TIC	204	0,75
Contra Constitución	Discriminación a través TIC (art. 510)	87	0,32
Otros		78	0,29
Total.		27.104	100,00

8.2.1 Procedimientos por delitos de estafa o defraudación

Como ya se ha venido observando en anteriores periodos anuales, el volumen más elevado de incoaciones corresponde a los procedimientos que tuvieron por objeto acciones ilícitas *online* encuadrables en la categoría de estafas o defraudaciones en sus diversas manifestaciones, que sumaron un total de 22.614, lo que supone un 83,43% del total de causas iniciadas en el año 2024 por cualquier clase de ciberdelito. Esta cifra da cuenta de un repunte de poco más del 16% –3.150 expedientes en números absolutos– en relación con la anualidad precedente y de un 12,45% respecto del año 2022, en el que el número de causas incoadas por este tipo de delitos fue de 20.111.

El incremento constatado en esta última anualidad puede tener su justificación, al menos en parte –y a ello se refieren varios de los delegados en sus respectivos informes– en la modificación de los artículos relativos a los delitos de estafa y defraudación, realizada por la Ley Orgánica 14/2022, de 22 de diciembre, que incorporó al Código Penal español la Directiva (UE) 2019/713 sobre lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. Con ocasión de esta reforma el legislador, al establecer la sanción correspondiente a las conductas típicas definidas en el vigente artículo 249 CP, ha prescindido de la cláusula tradicional en el derecho patrio según la cual si

la cuantía de la defraudación es inferior a 400 euros la conducta tiene el carácter de delito leve, manteniéndola exclusivamente en el artículo 248 CP en referencia a las estafas basadas en el engaño a la víctima. Dicha modificación legislativa en no pocos supuestos implica la posibilidad de utilizar, previa autorización judicial, medidas de investigación más invasivas y hasta el momento limitadas –en aplicación de criterios de proporcionalidad– respecto de delitos de carácter leve, lo que ha dado lugar a un aumento en el volumen de investigaciones por esta clase de ilícitos que son trasladadas a los órganos de la jurisdicción penal y por ello computadas en nuestras estadísticas.

No obstante, este elevado índice porcentual no tiene su justificación exclusivamente en el efecto derivado de la citada reforma legislativa, sino que también influyen en ello otras circunstancias. De hecho, esa elevadísima incidencia en el cómputo total de procedimientos iniciados anualmente por ciberdelitos se viene reflejando desde hace años en sucesivas memorias, con porcentajes ligeramente superiores en cada periodo. Así, si en el año 2020 el porcentaje correspondiente a las causas relativas a estos ilícitos fue del 72,43%, en las sucesivas anualidades se ha ido elevando en mayor o menor medida, pero en cualquier caso en forma progresiva y constante al 75,5% en 2021, 81,68% en 2022 y 82,87% en 2023, hasta alcanzar una cifra superior al 83% en el año memorial. También los sucesivos informes del Ministerio del Interior reflejan esta persistente y rápida tendencia alcista, de la que se ofrece un excelente indicador en el último Balance de Criminalidad correspondiente al año 2024 según el cual entre los años 2016 y 2024 las investigaciones policiales por ciberfraudes y/o ciberestafas se han incrementado en un 490,1%.

Como ya venimos indicando en las memorias de años precedentes, al analizar estas cifras han de tenerse en cuenta determinados factores que se mantienen constantes en las sucesivas anualidades y que influyen necesariamente en dichos resultados. En primer término, es evidente que se trata de acciones delictivas en las que –a diferencia de lo que acontece con otro tipo de conductas ilícitas que no afloran con facilidad– los y las perjudicados perciben claramente y denuncian con relativa frecuencia y, por ello, tienen puntual reflejo en nuestras aplicaciones informáticas. Pero, además, no es infrecuente que un número no precisado de dichas denuncias se refieran a efectos parciales de una misma actividad ilícita de forma tal que, si la investigación se realiza en forma adecuada, resultan finalmente acumuladas en un único procedimiento judicial, pese a lo cual, a efectos estadísticos, se mantienen los registros inicialmente efectuados. A estas circunstancias, suficientes por sí mismas para matizar las elevadas cifras que ofrece-

mos, se une la propia categorización de actividades ilícitas en nuestro CP que, en los arts. 248 y ss. tipifica como delitos de estafa una gran diversidad de conductas ilícitas que, aun respondiendo a idéntica finalidad defraudatoria, su planificación y ejecución se lleva a efecto en modalidades muy diferentes.

En todo caso, se trata de actuaciones delictivas que se han visto extraordinariamente facilitadas por las posibilidades de acción que ofrecen las TIC y que están produciendo gravísimos perjuicios económicos en nuestro país y a nivel mundial y, por ello, generan una especial atención por parte de los Gobiernos de la mayoría de los Estados. No solo se percibe con claridad su llamativo incremento cuantitativo sino también una rapidísima variación en las dinámicas criminales como consecuencia del aprovechamiento en la acción ilícita de las posibilidades que proporcionan los avances técnicos y científicos y, por ende, una evolución constante en los medios y formas de comisión.

Así, de un lado siguen siendo habituales las estafas de carácter tradicional basadas en el engaño, en las que el delincuente se sirve del elevado nivel de conectividad social para hacer llegar la superchería a un mayor número de víctimas, mejorando de esta forma sus ilícitos beneficios. Tal es el caso de la publicitación a través de foros chats o sitios webs –Mil Anuncios, Wallapop, etc.– de ofertas fraudulentas de todo tipo de bienes y servicios con la finalidad de captar la voluntad de la víctima y determinarla a realizar un desplazamiento patrimonial en su perjuicio. Las variantes son muy diversas y se hacen depender de las circunstancias del momento en que se desarrolla la acción criminal: alquileres de vivienda, ventas de entradas para conciertos y espectáculos públicos, viajes de vacaciones, etc. Son supuestos en los que normalmente la oferta engañosa se difunde en foros abiertos y de forma genérica e indiscriminada para hacerla llegar al mayor número posible de internautas y, solo en casos puntuales la superchería se articula de forma específica respecto de personas previamente seleccionadas *(spear phising).*

En los últimos años han proliferado las estafas de inversión en las que el defraudador capta a sus víctimas anunciando en la red la oportunidad de realizar aportaciones económicas, ya sea en moneda de curso real, en valores o en criptomonedas, a través de plataformas supuestamente dedicadas a actuaciones económicas o financieras aparentemente muy seguras y de muy alta rentabilidad, logrando de esta forma importantes desembolsos económicos por parte de las personas afectadas que los delincuentes hacen propios en su beneficio. Habitualmente las inversiones solicitadas inicialmente son de escasa entidad, haciendo creer a la víctima –en ocasiones a través de sofisticadas

demostraciones visuales– que la operación está generando pingues beneficios y provocando de esta forma nuevas entregas económicas, cada vez más sustanciosas, que posteriormente resultan irrecuperables. Aunque las variantes son muchas, son bastante frecuentes las que se sirven de las monedas virtuales –ya sea como reclamo para captar la voluntad de los internautas o como medio para facilitar el blanqueamiento de los beneficios así obtenidos– dada la complejidad que puede entrañar el seguimiento en la *blockchain* de las operaciones transaccionales y la identificación de sus autores. No obstante, ha de reconocerse que el reciente desarrollo legislativo en esta materia –Real Decreto-ley 7/2021, de 27 de abril, Reglamento Mica (UE) 2023/1114, de 31 de mayo y Real Decreto 249/2023, de 4 de abril, entre otros– está contribuyendo a mejorar las posibilidades de investigación de estos comportamientos, al imponer a los proveedores de servicio que actúan como intermediarios en las operaciones de criptoactivos y/o en la custodia de las *wallets* determinadas obligaciones de control y traslado de información que son de especial utilidad a estos efectos. En otras ocasiones, se recurre a mecanismos como el *phishing* o *smishing* –envío de mensajes fraudulentos a través de la red o mensajes de texto con enlaces engañosos– o incluso al empleo de comunicaciones telefónicas, *vishing,* para engañar a la víctima simulando representar a empresas, entidades o incluso a instituciones públicas mediante la manipulación del identificador de la línea llamante o de los mensajes cortos SMS o MMS, todo ello con el objetivo de obtener sus datos personales o bancarios y emplearlos posteriormente para realizar desplazamientos patrimoniales en su perjuicio. La frecuencia creciente de este tipo de actuaciones y su repercusión no solo en las personas afectadas directamente por ello sino también en la necesaria confianza de la ciudadanía en las comunicaciones electrónicas y en la actividad comercial o mercantil *online*, han determinado en nuestro país la publicación de la Orden Ministerial TDF/149/2025, de 12 de febrero, que impone a los operadores de comunicaciones la obligación de bloquear aquellas llamadas o mensajes cortos que presenten signos de manipulación o de origen dudoso. También es cada vez más frecuente el apoderamiento con finalidad defraudatoria de datos personales ajenos, a través del acceso irregular a bases y sistemas de almacenamiento, actuaciones que, dada su naturaleza, analizaremos juntamente con los delitos de ataques a sistemas informáticos.

La simulación de la identidad de otras personas para la ejecución de actuaciones fraudulentas se detecta también con asiduidad en operaciones de la banca *online*. El recurso a las TIC para actuaciones tales como la apertura de cuentas bancarias, la solicitud de préstamos o la

ordenación de transferencias en las que no es posible la comprobación directa y presencial de quien efectivamente realiza la operación, se ha ido extendiendo rápidamente entre los clientes de las entidades bancarias, lo que está incrementando seriamente el riesgo de usurpación de identidades ajenas, con el perjuicio que esta situación puede generar para el afectado. Por ello, las actuaciones que se están llevando a efecto por dichas entidades para invitar e, incluso, estimular a sus clientes a realizar *online* ese tipo de actuaciones debería ir acompañada necesariamente de la adopción por su parte de las medidas de seguridad imprescindibles para evitar dicho riesgo, asumiendo en caso contrario las consecuencias perjudiciales que pudieran derivarse para quienes resulten afectados.

Otra modalidad delictiva que está generando gravísimos perjuicios, particularmente en el sector empresarial, dando lugar a la incoación y tramitación en nuestro país de un volumen significativo de procedimientos, es la conocida como fraude BEC *(Business Email Compromise).* En estos supuestos, el sujeto activo se hace pasar por algún directivo de la empresa (CEO) o alguien de confianza en el marco de su actividad cotidiana, tal como un proveedor o un cliente habitual y, con esa engañosa cobertura, se dirige a quien se encuentra habilitado en la entidad para llevar a efecto las gestiones económicas y le determina a ordenar un desplazamiento patrimonial a su favor. Se trata de actuaciones en las que se combina el engaño –como elemento básico de la estafa tradicional– con la manipulación informática, ya que en muchas ocasiones es necesario el previo compromiso del correo electrónico, o el uso de otra técnica similar, para adquirir el conocimiento imprescindible sobre el funcionamiento de la empresa que permita articular la superchería.

No podemos tampoco dejar de mencionar, aunque sea brevemente, las acciones fraudulentas vinculadas al uso irregular de instrumentos de pago distintos del efectivo, dado el volumen especialmente importante de investigaciones que generan, aun cuando muchas de las cuales no llegan a ser trasladadas a los órganos de la jurisdicción penal –en atención a lo dispuesto en el artículo 284 LECrim– y por tanto carecen de reflejo en las estadísticas judiciales o del Ministerio Fiscal por las dificultades que presenta su investigación así como la determinación de sus autores como consecuencia de la posibilidad de utilizar estos instrumentos de pago *online* en cualquier lugar del mundo. No obstante, la redefinición de esta figura delictiva en el artículo 249 1b y 2b CP, por mor de la reforma operada en dicho texto legal por la LO 14/2022, de 22 de diciembre, ha hecho aflorar algunas novedosas modalidades de defraudación mediante el uso irregular de instrumen-

tos de pago de carácter inmaterial, tales como las relacionadas con las aplicaciones de pago móvil o el *bizum inverso,* que están siendo objeto de investigación en procedimientos judiciales incoados en distintos lugares del territorio nacional.

El alcance de la influencia que pueda llegar a tener en la actividad defraudatoria el empleo de sistemas de inteligencia artificial es todavía difícil de predecir. Por el momento ya se han incoado un buen número de procedimientos en los que la capacidad de engañar a la víctima se ha visto considerablemente mejorada por la intervención simulada, mediante IA, de personas que pueden ejercer sobre ella una mayor influencia. Buen ejemplo de ello son actuaciones como «la estafa del hijo en apuros» o aquellas otras que se sirven de la imagen audiovisual falseada de un personaje conocido y/o famoso en el ámbito de la política o las finanzas. También nos consta la utilización de los sistemas IA para detectar las vulnerabilidades de los sistemas informáticos y poder planificar con mayor seguridad y rapidez determinados ataques o acciones de fraude informático. En cualquier caso, se trata de una materia que por su novedad está siendo objeto de especial atención para la Red de fiscales especialistas, no solo en acciones formativas sino también mediante el constante intercambio de experiencias y conocimientos, entre nosotros y con las Fuerzas y Cuerpos de Seguridad, a efectos de poder responder de forma efectiva frente a estas nuevas situaciones.

8.2.2 Ataques a sistemas informáticos

Los procedimientos incoados por ataques a sistemas informáticos, ya se incardinen en los arts. 197 bis y ter o en los arts. 264 y ss. CP, mantienen un número de registros muy similar al del año precedente, con 93 incoaciones (0,34 % del total) en el primer caso y 137 (0,51% del total) en el segundo.

Las cifras poco relevantes que ofrecemos en este apartado no deben restar importancia a estas agresiones cuya entidad y efectos lesivos resultan cada vez más preocupantes. Además, en lo que se refiere a las del primer grupo ha de recordarse que se trata de agresiones vinculadas en no pocas ocasiones a acciones que atentan contra la intimidad de las personas o, en su caso, contra el secreto y confidencialidad en el ámbito empresarial y, por tanto, también encuadrables respectivamente en los arts. 197.1 y 2 y 278 y ss. del CP, lo que determina que, en un número no precisado de supuestos, las conductas de acceso ilegal a sistemas informáticos no sean objeto de registro inde-

pendiente sino que queden absorbidas por la anotación correspondiente a estos últimos ilícitos. Por ello es de interés reseñar que los delitos contra la intimidad antes indicados dieron lugar a la incoación de 443 procedimientos en 2024 –un 1,63% del total– con un incremento de poco más del 12 % respeto del año 2023, en tanto que los delitos de descubrimiento y revelación de secretos de empresa generaron únicamente 23 nuevos registros.

Nuestra experiencia en la investigación de estas conductas nos ha permitido constatar que sus manifestaciones en términos generales obedecen a dos tipos de dinámicas delictivas claramente diferenciadas tanto en su finalidad como en la forma de planificar y desarrollar el *iter criminis*, aunque su calificación jurídica sea inicialmente similar. De un lado, aquellos supuestos más tradicionales en los que el agresor conoce previamente a la víctima y, por razones diversas, accede irregularmente a información privada sobre la misma que se encuentra almacenada en sistemas o bases de datos. Tal es el caso de los actos de apoderamiento o conocimiento no autorizado de datos relativos a la salud de las personas que se conservan en los centros médicos u hospitalarios o de la información alojada en bases de datos policiales u otro tipo de registros de entidades públicas o privadas o, también, de la intrusión no consentida en un dispositivo móvil o en el correo electrónico de otro con ese mismo objetivo. Junto a estas modalidades de invasión en la intimidad ajena, en los últimos años se han venido detectando otro tipo de agresiones en las que el acceso a contenidos, contraseñas o a los datos personales de terceros se realiza de forma masiva e indiscriminada, generalmente por parte de grupos organizados de carácter internacional, con la finalidad de utilizar posteriormente la información así obtenida con objetivos ilícitos diversos y, en muchas ocasiones, para la ejecución de actividades de carácter defraudatorio.

Son estas últimas las que están generando una mayor preocupación social, no solo por la frecuencia con la que se producen sino también por la creciente sofisticación en su planificación y ejecución, por su dimensión internacional y porque el volumen de datos exfiltrados llega a alcanzar dimensiones significativas de modo tal que afectan o ponen en riesgo los derechos de un número creciente de ciudadanas/os. Así ha ocurrido con los ataques acaecidos en 2024 dirigidos, entre otros, contra el Banco Santander, Iberdrola o la DGT que dejaron expuestos datos correspondientes a muchos usuarios o clientes de dichas entidades. A nivel mundial, resultaron de especial relevancia los ataques que tuvieron por objeto la exfiltración de información de la entidad tecnológica Finastra o de la red de transportes de Londres.

Por su parte, en lo que se refiere a los ataques de sabotaje informático las modalidades más frecuentes son los ataques DDoS y el *ransomware,* tipo de *malware* o código malicioso que, una vez introducido en el sistema informático afectado, impide su funcionamiento ya sea cifrando la información o bloqueando la pantalla y priva a los usuarios del acceso total o parcial a los datos almacenados, a los programas o al sistema en su conjunto. Normalmente, el objetivo de los atacantes es obtener un beneficio económico por lo que una vez ejecutado suelen reclamar a la víctima el pago de un rescate para recuperar la disponibilidad de la información. No obstante, las variantes son muchas y, en ocasiones, la agresión inicial se acompaña de la exfiltración de los contenidos alojados en el sistema atacado y, en su caso, de la amenaza de su publicación posterior si no se efectúa un nuevo desplazamiento patrimonial, circunstancia que se conoce como *doble extorsión.*

Aunque la respuesta penal a este tipo de fenómenos es muy compleja y normalmente exige el recurso a medidas de cooperación internacional, se va produciendo un lento, aunque constante incremento en el número de incoaciones por hechos ilícitos de esta naturaleza que obedece, al menos en parte, a una adecuada coordinación con las entidades responsables en la prevención y detección de estas conductas. Nos referimos a las comunicaciones que efectúa la Oficina de Coordinación de Ciberseguridad (OCC) a las Fuerzas y Cuerpos de Seguridad y a esta Unidad de Criminalidad Informática de la FGE dando cuenta de aquellos incidentes de seguridad que llegan a su conocimiento y presentan caracteres de delito y a las que se acompaña la información y evidencias relacionadas con dichos incidentes. Estas comunicaciones, efectuadas al amparo de lo establecido en el artículo 14.3 del Real Decreto-ley 12/2018, de 7 de septiembre, que incorporó al ordenamiento interno la Directiva (UE) 2016/1148, de 6 de julio, sobre seguridad de las redes y sistemas de información, constituyen la base para iniciar, si así se estima procedente, las investigaciones criminales que, en su caso, darán lugar a la correspondiente actuación penal frente a los responsables de estas conductas. De esta forma se complementa la acción preventiva con la acción sancionadora del Estado frente a estos graves comportamientos.

En relación con unos y otros ataques informáticos estimamos necesario llamar la atención sobre dos aspectos de significativa relevancia y que desde nuestro punto de vista habrían de ser tenidos en cuenta en la actuación futura frente a dichos comportamientos e incluso en las decisiones de política criminal que hayan de adoptarse.

El primero de ellos relativo a la proliferación en el entorno tecnológico del modelo criminal conocido como *Crime as a Service,* caracterizado por la actuación de grupos u organizaciones criminales que se han ido especializando en la prestación u oferta a los restantes usuarios de la red de plantillas, infraestructuras, servicios o productos –tales como contraseñas, bases de datos sustraídas, técnicas de *hacking,* control remoto de dispositivos, *malware* para ataques de *ramsomware* o DDoS, etc.– específicamente diseñados y preparados para la ejecución de actividades ilícitas, ya se trate de fraudes o de delitos informáticos de distinta naturaleza como los ciberataques o los actos de ciberterrorismo. En definitiva, se está generado un comercio criminal internacional que permite a sus artífices obtener pingues beneficios por la mera puesta a disposición de terceros de herramientas de piratería que hacen posible desarrollar acciones delictivas *online*, aun careciendo de conocimientos informáticos. El crecimiento imparable de estas innovadoras formas de delincuencia, su peligrosidad y naturaleza transnacional, las dificultades que entraña su localización en el ciberespacio y su desarticulación, el riesgo que conllevan sus actuaciones junto con la relevancia de estos servicios para la efectividad de la finalidad ilícita pretendida, suscitan cuestiones jurídicas y técnicas de interés que pudieran determinar la necesidad de incorporar y/o modificar tipos penales o, incluso, de definir nuevas herramientas de investigación criminal.

La segunda cuestión que estimamos necesario destacar es la detección, en los últimos meses, de algunas agresiones informáticas que, por la forma de manifestarse y el tipo de objetivos atacados, llevan a considerar que su finalidad no es tanto la obtención de beneficios de carácter patrimonial o la causación de un perjuicio concreto a un tercero –como en los supuestos anteriormente referidos– sino la de desestabilizar la actividad ordinaria de entidades oficiales, instituciones o influir en la toma de decisiones de los poderes públicos. Tal es el caso, entre otras, de determinadas agresiones que, coordinadas desde el extranjero pero contando ocasionalmente con apoyo en el propio territorio del Estado, difunden deliberadamente informaciones falsas y/o atacan los mecanismos establecidos para el control y seguimiento de procesos electorales o las páginas web y aplicaciones de altas instituciones y organismos implicados en la seguridad del Estado con el objetivo de perturbar el desempeño de sus funciones, desacreditarlos o simplemente como forma de coacción o de «castigo» por determinadas decisiones o actuaciones adoptadas en el marco de las relaciones con otros Estados o con los organismos internacionales.

Las especiales connotaciones de este tipo de agresiones, y la posibilidad de encuadrarlas en alguno de los tipos penales competencia de la Audiencia Nacional, está determinado un cuidadoso seguimiento y control de su investigación por parte de esta Unidad especializada en coordinación constante y directa con las fuerzas policiales y la Fiscalía del citado órgano jurisdiccional.

8.2.3 Delitos contra bienes personalísimos

En el apartado de ilícitos contra la intimidad personal, además de los 443 expedientes por delitos de los arts. 197.1.º y 2.º CP, a los que antes nos hemos referido por su posible vinculación con los ataques informáticos, se han de incluir los 107 relativos a supuestos de difusión no autorizada de imágenes íntimas obtenidas con el consentimiento de la víctima. Ello implica un total de 550 registros, lo que supone un índice porcentual del 2,02% del total por ciberdelitos y un incremento de casi el 12% respecto de las 492 investigaciones judiciales por ilícitos de esta naturaleza registradas en el año 2023. Además de las conductas de acceso irregular a información íntima alojada en dispositivos informáticos, a las que ya nos hemos referido a propósito de los ataques a sistemas informáticos, se encuadran también en este apartado los procedimientos relativos a la obtención subrepticia de imágenes o contenidos auditivos a través de la instalación de cámaras de grabación en espacios privados o mediante la activación a distancia de los mecanismos establecidos con esa misma finalidad en los dispositivos móviles.

Por su parte, los delitos contra la libertad y seguridad de las personas determinaron en el pasado año un total de 1.846 procedimientos, un 6,8% del conjunto de incoaciones por ciberdelitos. Esta cifra, ligeramente superior –en un 12%– respecto del resultado obtenido en el año anterior, es el reflejo del crecimiento lento pero constante de este tipo de acciones ilícitas en el entorno *online* derivado del incremento de la conectividad y el traslado de todo tipo de relaciones interpersonales a la red. El número más elevado es el correspondiente a las ciberamenazas, con un 5,64% del total, en tanto que las conductas de acoso permanente u hostigamiento, sancionadas en el artículo 172 ter CP, supusieron solo el 1,17%. Ciertamente, una buena parte de los delitos contra la libertad y seguridad de las personas se producen en el entorno físico y otros muchos se enmarcan en el ámbito de la violencia de género y, en consecuencia, se registran en dicha área de especialización sin reflejo en nuestras estadísticas

de criminalidad informática. En consecuencia, los datos que ofrecemos únicamente pretenden dar cuenta de aquellas actividades de esta naturaleza, cualesquiera que sean los implicados como sujeto activo y pasivo, en las que el empleo de las tecnologías haya resultado determinante ya sea en la planificación o en la ejecución de la actividad criminal.

Dentro de los procedimientos relativos a los delitos contra bienes personalísimos es también obligada la referencia a los que tienen por objeto atentados contra la integridad moral, que en la pasada anualidad sumaron 54 incoaciones, 9 menos que en 2023. También en este caso, hemos de hacer la salvedad de que únicamente se registran como tales en las secciones de criminalidad informática aquellos en los que el trato degradante a la víctima se lleva a efecto a través de las TIC. Entre ellos, se han incluido en este apartado algunos procedimientos incoados como consecuencia de la distribución en el entorno virtual de contenidos de carácter íntimo o sexual elaborados mediante sistemas de Inteligencia Artificial en los que aparecen representadas personas mayores de edad y fácilmente identificables cuya dignidad se ha visto profundamente afectada como consecuencia de dicha actuación. Se trata de conductas que, aunque por el momento no están tipificadas de forma expresa, a nuestro entender encajan perfectamente en artículo 173 CP al incidir en el bien jurídico que nos ocupa. De hecho, en la propuesta remitida recientemente por el Gobierno al Parlamento para la aprobación, en su caso, de una ley orgánica sobre protección integral de los menores en los entornos virtuales se definen como delito estas conductas en el proyectado artículo 173 bis, cuya incorporación se pretende efectuar en el capítulo dedicado a la protección de este mismo bien jurídico, lo que consideramos corrobora nuestra valoración acerca de los intereses afectados por estas acciones.

8.2.4 Delitos contra la libertad sexual

Otro capítulo de indiscutible interés en esta Memoria es el correspondiente a los expedientes incoados por ilícitos *online* contra la libertad sexual que, aunque en principio pueden llevarse a efecto respecto de cualquier persona, en su mayoría, dadas las especiales connotaciones de estas conductas, suelen afectar a menores de edad.

Antes de analizar detalladamente los datos recopilados al respecto, es de interés destacar que, por las características propias de este tipo de investigaciones, no es infrecuente que sobre la base de una previa

denuncia por un ilícito de esta naturaleza se proceda al registro de los dispositivos del investigado y a la incautación y posterior análisis de todo el material ilícito que tenga a su disposición, ya sea en terminales físicos o en la nube. Con bastante frecuencia ello determina la incoación de un solo procedimiento para el esclarecimiento de todos los ilícitos que le son imputables a una misma persona a consecuencia de las evidencias localizadas con ocasión de una única actuación policial o judicial. Por otra parte, en no pocas ocasiones, el agresor va realizando de forma sucesiva distintas conductas sobre la víctima –todas ellas ilícitas e inspiradas en una misma intención criminal, causándole de esta forma un gravísimo efecto lesivo– ya se trate de *child grooming;* agresión sexual física o virtual y elaboración y/o, en su caso, distribución de material de abuso sexual infantil, siendo todas ellas objeto de indagación en el mismo procedimiento. Esto explica que, en estas causas, a diferencia de otro tipo de investigaciones, en un mismo expediente se investigue y, en su caso, se formule acusación y enjuicie a una persona por una diversidad de actividades delictivas, encuadrables en distintos tipos penales y desarrolladas en un periodo temporal más o menos amplio, las cuales pueden afectar no solo a una víctima sino a varias de ellas, en ocasiones, en número significativamente elevado.

Adelantamos este comentario para explicar las cifras estadísticas que ofrecemos, que pueden parecer de escasa importancia, especialmente si las comparamos con otras más abultadas, como es el caso de las estafas o defraudaciones, pero que dan cuenta de procedimientos en los que en muchas ocasiones en una sola causa se investigan y enjuician una pluralidad de delitos. Y esta circunstancia afecta no solo al volumen total de ilícitos investigados sino también a su categorización por tipos penales ya que, al efectuarse la anotación registral por una sola figura delictiva –ordinariamente la más grave– quedan al margen del cómputo otras conductas ilícitas incardinables en otros tipos penales que también son objeto del mismo procedimiento.

Con estas salvedades, la información recopilada refleja la incoación de un total de 1.197 causas por ilícitos de esta naturaleza, lo que supone un escaso 4,41 % del total de registros por ciberdelitos en el año 2024. Con todo, estos resultados revelan un ligerísimo incremento del 4,8 % respecto de los 1.142 procedimientos incoados en 2023 y un descenso más acentuado, de aproximadamente el 20%, respecto de las cifras obtenidas por estos mismos conceptos en 2022 y en 2021. Es significativo que, pese al incuestionable y preocupante aumento de este tipo de conductas –avalado por serios y reiterados

indicadores nacionales e internacionales– el volumen de procedimientos incoados año a año por estas graves actuaciones delictivas se mantenga constante con ligeras oscilaciones. En ello influyen, sin duda, las imprecisiones en los registros y anotaciones estadísticas antes apuntadas, pero también las circunstancias inherentes a la propia actividad delictiva, que dificultan el afloramiento de estas conductas y la posibilidad de que lleguen a conocimiento de los cuerpos policiales o de los órganos de la jurisdicción penal. Ello es así porque son acciones criminales que se planifican y ejecutan en la intimidad y que muy difícilmente son denunciadas por las propias víctimas ya que frecuentemente son niños o niñas de tan corta edad que, o bien no son conscientes de que están siendo víctimas de una agresión, o bien se encuentran intimidados, engañados o coaccionados por el propio agresor y/o en una especial situación de vulnerabilidad por su situación de dependencia o vinculación afectiva o económica con el mismo. La denuncia suele llegar a nuestro conocimiento por sospechas de los padres o tutores al detectar reacciones anómalas en su hijos o pupilos o, más frecuentemente, por denuncias de usuarios de la red o por informaciones recibidas a través de organismos internaciones o de cuerpos policiales de otros países que, en sus propias investigaciones, detectan direcciones IP, geolocalizadas en España, que parecen ser el origen de algunas de estas conductas. Pero se trata de comunicaciones o denuncias puntuales que no se corresponden con el preocupante aumento de este tipo de agresiones en el entorno virtual y cuyo volumen únicamente podemos intuir a partir de informaciones obtenidas por vías indirectas y circunstanciales, como los reportes de los proveedores de servicios sobre tráfico de material CSAM en la red y los informes de organizaciones internacionales.

Son conductas, además, muy peligrosas por afectar a bienes jurídicos extraordinariamente sensibles y cuyo efecto lesivo puede ser cada vez más grave dadas las posibilidades que ofrecen las TIC para la realización de todo tipo de acciones *online* de contenido sexual, incluidas las agresiones con introducción de objetos o la convocatoria y celebración de espectáculos pornográficos con intervención de menores que son visionados en *streaming* por cientos de personas ubicadas en lugares distintos y distantes, más allá de los límites fronterizos de los Estados.

Pero, además, se trata de actividades delictivas cuya investigación ofrece dificultades cada vez mayores como consecuencia de los avances técnicos y científicos y, con ellos, de la propia evolución en las formas y medios de contactar y mantener relaciones con las víctimas

o, en su caso, de elaborar, difundir o consumir material de abuso. La encriptación de las comunicaciones y de los sistemas de mensajería instantánea, el consumo en *streaming* de material de abuso o las facilidades que ofrece la red para el anonimato son circunstancias que dificultan las posibilidades de actuación frente a estos comportamientos. Por otra parte, las capacidades que ponen a disposición de cualquier persona los sistemas de inteligencia artificial para elaborar con facilidad material CSAM, en condiciones de realismo adecuadas para proporcionar apariencia de veracidad a dichos contenidos y, en consecuencia, poder distribuirlos como tal en el entono virtual, está contribuyendo a promover y fomentar el comercio ilícito de esos peligrosos materiales y de prácticas especialmente dañinas que suponen un riesgo serio y efectivo para el normal desarrollo y evolución de la infancia y adolescencia, lo que hace imprescindible una respuesta contundente desde el Estado de Derecho.

Por ello, merece una valoración muy positiva la iniciativa legislativa del Gobierno para mejorar la protección de los menores en el entorno digital al igual que la reforma en la que se está trabajando en la Unión Europea para la adecuación de las medidas previstas en la Directiva (UE) 2011/93 a las nuevas formas de agresión contra estos bienes jurídicos. Así mismo, debe fomentarse la denuncia ciudadana de estas conductas, ya sea en forma directa a las fuerzas y cuerpos policiales, ya sea a través de las *hotline* articuladas con dicha finalidad, particularmente la gestionada por INHOPE cuyos resultados para España gestionamos en la Unidad Especializada en colaboración directa con el Instituto Nacional de Ciberseguridad (INCIBE) y con los cuerpos policiales.

Finalmente, a efectos de completar la información estadística que incorporamos en la tabla correspondiente, hemos de indicar que los procedimientos computados como «otros» son los incoados por ilícitos no reseñados específicamente en la misma, tales como los relativos al incumplimiento por medios tecnológicos de medidas de aproximación y/o acercamiento, el blanqueo de capitales o la extorsión. Entre ellos se destaca por su novedad algún procedimiento incoado por delito del artículo 361 bis CP relativo a conductas de riesgo que pueden generar trastornos alimentarios.

8.2.5 Escritos de acusación

Los datos relativos a los escritos de acusación presentados por el Ministerio Fiscal durante el año memorial ofrecen a nuestro enten-

der una información especialmente valiosa a efectos de dejar constancia de aquellos supuestos en los que la Fiscalía, una vez culminado el proceso de investigación y en atención a las pruebas practicadas y su resultado, considera que dispone de evidencias suficientes para formular acusación contra persona o personas concretas, por considerarla/s responsables de hechos perfectamente definidos y encuadrables en alguno de los ilícitos que sanciona nuestro Código Penal. Se trata, por tanto, de una información generada por la propia Institución como resultado del estudio serio y reflexivo, tanto fáctico como jurídico, de los múltiples procedimientos en los que tenemos intervención. Obviamente, las cifras que ofrecemos por este concepto son más reducidas que las que resultan del análisis de la incoación de nuevos expedientes y su utilidad a efectos de valorar la evolución de la ciberdelincuencia es menor. No obstante, constituyen en sí mismas un excelente parámetro para reflexionar acerca de la eficacia de la investigación policial y judicial frente a este fenómeno criminal y también sobre la capacidad de respuesta desde el Estado de Derecho y las carencias detectadas y las posibles vías de actuación futura.

Según los datos remitidos por los órganos territoriales, en el año 2024 el Ministerio Fiscal formuló 4.406 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 (arts. 169 y ss y 172 y ss)	243	5,52
	Acoso a través de TIC (art. 172 ter)	96	2,18
Contra la integridad moral	Trato degradante a través de TIC (art. 173)	11	0,25
Contra la libertad sexual	Pornografía infantil/discapacidad a través de TIC (art. 189)	353	8,01
	Acoso menores a través de TIC (art. 183 ter)	70	1,59
	Otros delitos c/libertad sexual a través TIC	323	7,33
Contra la intimidad	Ataques/interceptación sistemas y datos (art. 197 bis y ter)	6	0,14
	Difusión inconsentida de imágenes íntimas (art. 197.7)	18	0,41
	Descubrimiento/revelación secretos a través TIC (art. 197)	120	2,72

Delitos informáticos		Calificaciones	%
Contra el honor	Calumnias/injurias autoridades a través TIC (art. 215)	10	0,23
Contra el patrimonio y el orden socioeconómico	Estafa cometida a través de las TIC (art. 248 y 249)	2.967	67,34
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss)	12	0,27
	Delitos c/ servicios de radiodifusión/interactivos (art. 286)	14	0,32
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	18	0,41
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss)	12	0,27
De falsedad	Falsificación a través de las TIC	46	1,04
Contra Constitución	Discriminación a través TIC (art. 510)	18	0,41
Otros		69	1,57
Total		4.406	100,00

La cifra total de acusaciones refleja un significativo repunte, de un 22,97% respecto del año 2023 y un 7,75% respecto del año 2022. Quiere decirse con ello que, al igual que indicábamos respecto a la evolución en el número de procedimientos por ciberdelitos, la leve inflexión detectada en los años 2022 y 2023 no tiene entidad suficiente para cuestionar la tendencia claramente ascendente que también en este aspecto venimos observando desde el inicio de nuestra actividad como área de especialización en 2011. Así, tomando como referencia el año 2016, primera anualidad completa de vigencia de la importante reforma operada por la LO 1/2015 en materia de cibercrimen, los resultados que hemos ido obteniendo revelan un incremento de un 167,35% en el número de escritos de acusación por ciberdelitos formulados por la Fiscalía en estos últimos 9 años que se concreta en cifras absolutas en la forma siguiente:

Año 2016	Año 2017	Año 2018	Año 2019	Año 2020	Año 2021	Año 2022	Año 2023	Año 2024
1.648	1.715	1.955	2.847	3.027	4.104	4.089	3.583	4.406

Como resulta del análisis de la tabla adjunta, el porcentaje más elevado de acusaciones corresponde a las formuladas por delitos de estafa y defraudación, que ascendieron a 2.967, un 67% del total. Respecto del año 2023, se detecta un significativo incremento de casi un

37% que al menos en parte puede estar motivado por la circunstancia de que las conductas ilícitas encuadrables en el artículo 249 CP, tras la reforma operada por la LO 14/2022, tengan la consideración de delito menos grave cualquiera que sea la cuantía de la defraudación y, por ello, den lugar a la presentación de escritos de acusación.

Le siguen en importancia las acusaciones por delitos *online* contra la libertad sexual, que sumaron un total de 746, un 16,93 % del total, siendo las más numerosas las relativas a la elaboración o puesta a disposición de terceros de material CSAM que ascienden a 353, un 8,01% de las presentadas en el año por ciberdelitos. Por su parte, en el apartado correspondiente a otros delitos contra este mismo bien jurídico, que ascienden a 323, se incluyen las formuladas por cualesquiera otras de las actividades delictivas de similar naturaleza –salvo el *child grooming* que es objeto de cómputo independiente– entre ellas las agresiones sexuales *online*, las conductas de inducción a menores en la prostitución o las de exhibicionismo. En el año 2023 los escritos de acusación por delitos *online* contra la libertad sexual por todos los conceptos fueron 544, lo que da cuenta de un incremento en el año memorial de algo más del 37%. Al igual que comentábamos a propósito de los procedimientos incoados en el año, en la mayoría de estos escritos la acusación se formula por una diversidad de actos delictivos y respecto de una pluralidad de víctimas, pese a lo cual su reflejo estadístico, por las razones anteriormente indicadas, suele concretarse en una única anotación.

Aunque la comparación entre los resultados obtenidos en este apartado y en el correspondiente a procedimientos incoados en el mismo periodo anual ha de tomarse con especial cautela, dado que las acusaciones formuladas en 2024 en su mayoría se refieren a procedimientos iniciados en anteriores ejercicios, dicha comparación ofrece una perspectiva, de incuestionable interés, acerca de nuestra capacidad de respuesta ante el fenómeno criminal que nos ocupa en su conjunto y en cada una de sus manifestaciones. Así, es llamativo que, en términos generales y con las salvedades antes indicadas, únicamente el 13% de las investigaciones judiciales por delitos de estafa o defraudación *online* culminen con la presentación de escrito de acusación por parte del Ministerio Fiscal, en tanto que en referencia a los ciberdelitos contra la libertad sexual dicho porcentaje se eleve hasta más del 62%. La explicación, que ya venimos avanzando en otros apartados de esta Memoria, ha de buscarse en las diferencias existentes en el origen y circunstancias de la propia investigación en función del tipo de delito a que se refiere. Así, en el caso de las estafas y defraudaciones la denuncia se presenta habitualmente por el propio perjudicado

que en muchas ocasiones carece totalmente de información sobre el responsable criminal que se habrá servido en su favor de cualquiera de los múltiples medios de anonimización disponibles en el entorno virtual. Por el contrario, en los supuestos de delitos sexuales las denuncias que se presentan suelen identificar al responsable criminal o, al menos, ofrecen información que lo hacen posible– como es el caso de las direcciones IP o perfiles de contacto– y lo mismo acontece con los reportes o notificaciones recibidos de terceros, lo que permite orientar favorablemente la investigación desde un inicio e incluso ampliarla posteriormente a otros hechos delictivos como consecuencia de la incautación en poder del agresor de material ilícito de diversa procedencia. Por su parte, los delitos contra la libertad y seguridad de las personas dieron lugar en 2024 a la presentación de 339 escritos de acusación, siendo los más numerosos los referentes a amenazas y coacciones que supusieron un 5,52% del total. A su vez, en referencia a los escritos contra la integridad moral, se formularon 11 acusaciones, alguna de ellas por la difusión de material de carácter íntimo y sexual elaborado mediante inteligencia artificial y relativo a personas perfectamente identificables.

En 2024 también se elaboraron por el Ministerio Fiscal 18 escritos de acusación por daños informáticos –una más que en 2023– y únicamente 6 por delitos de los artículos 197 bis y ter CP, si bien un número indeterminado de acusaciones por hechos de este tipo han podido quedar enmascarados en las anotaciones relativas a delitos de descubrimiento y revelación de secretos de los artículos 197. 1.º y 2.º CP que dieron lugar a la presentación de 120 escritos de esa naturaleza.

Finalmente, hemos de indicar que en el apartado «otros» se incluyen: 42 acusaciones por delitos de blanqueo de capitales; 4 por delitos de extorsión y 11 por conductas de quebrantamiento *online* de condena o medida cautelar.

8.2.6 Diligencias de investigación del Ministerio Fiscal

El objetivo de este apartado de la Memoria es analizar la actuación de la Red de fiscales especialistas y de la propia Unidad Especializada en las investigaciones relativas a ciberdelitos tramitadas directamente por la Fiscalía, 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 o comunicaciones remitidas por organis-

mos o instituciones públicas; testimonios de procedimientos judiciales; puesta en conocimiento de investigaciones de los Cuerpos y Fuerzas de Seguridad, o también denuncias remitidas por entidades de la sociedad civil o por particulares que, al amparo de los artículos 259 y ss. LECrim, trasladan directamente al Ministerio Fiscal información sobre determinados hechos o acontecimientos que consideran de carácter delictivo.

La apertura de estos expedientes supone la asunción directa por el Ministerio Fiscal de la actividad investigadora si bien con importantes limitaciones en un doble aspecto: temporal y objetivo. En cuanto al primero, porque el artículo 5 EOMF fija un plazo máximo para el desarrollo de estas actuaciones preprocesales –6 o 12 meses, según los casos– aunque se contempla la posibilidad de prórroga, que ha de acordarse por Decreto motivado del Fiscal General del Estado. Además, el segundo aspecto a destacar viene referido a que la capacidad de investigación de la Fiscalía tiene como límite constitucional la práctica de diligencias que, por incidir en derechos fundamentales de la persona investigada, requieren de autorización judicial, circunstancia que necesariamente determina el traslado de las actuaciones al órgano judicial competente para la prosecución de la investigación. Por razones obvias, en la materia que nos ocupa dicha circunstancia concurre con frecuencia ya que en la mayoría de las investigaciones por ciberdelitos resulta imprescindible realizar diligencias que pueden suponer una intromisión en la intimidad, el secreto de las comunicaciones o la protección de datos de carácter personal, lo que condiciona nuestra capacidad de actuación en el marco de estos expedientes.

Por otra parte, ha de indicarse que esta Unidad Especializada contra la Criminalidad Informática, por mor de lo dispuesto en la Circular 2/2022 de la FGE, tiene encomendada la facultad de incoar y tramitar diligencias de investigación penal –sin sujeción a previa autorización del Fiscal General del Estado– a los solos efectos de realizar todas las averiguaciones necesarias, que no requieran de orden judicial, para determinar el órgano del Ministerio Fiscal competente territorialmente para el conocimiento de los hechos investigados y también para solicitar, en su caso, la preservación de evidencias del proveedor de servicios que las tenga a su disposición. Estas actuaciones, atribuidas con carácter exclusivo a la propia Unidad, tienen por objeto colaborar con las restantes Unidades y órganos del Ministerio Fiscal en la concreción del *forum delicti comisi,* dadas las dificultades que ello puede entrañar cuando se trate de

actividades ilícitas planificadas y ejecutadas total o parcialmente en el entorno tecnológico.

El volumen de diligencias de investigación incoadas por la Fiscalía en el año memorial asciende a 444, cifra que refleja un ligero descenso, de un 11%, respecto de las 498 incoadas en 2023.

El análisis desglosado de estos expedientes es el siguiente:

Órganos territoriales

Delitos informáticos		Diligencias de investigación	%
Contra la libertad	Amenazas/coacciones a través de TIC (art. 169 y ss y 172 y ss)	10	3,12
	Acoso a través de TIC (art. 172 ter)	7	2,18
Contra la integridad moral	Trato degradante a través de TIC (art. 173)	1	0,31
Contra la libertad sexual	Pornografía infantil/discapacidad a través de TIC (art. 189)	38	11,84
	Acoso menores a través de TIC (art. 183 ter)	2	0,62
	Otros delitos c/libertad sexual a través TIC	8	2,49
Contra la intimidad	Ataques/interceptación sistemas y datos (art. 197 bis y ter)	4	1,25
	Difusión inconsentida de imágenes íntimas (art. 197.7)	6	1,87
	Descubrimiento/revelación secretos a través TIC (art. 197)	29	9,03
Contra el honor	Calumnias/injurias autoridades a través TIC (art. 215)	12	3,74
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TIC (art. 248 y 249)	42	13,08
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss)	2	0,62
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	7	2,18
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss)	1	0,31
De falsedad	Falsificación a través de las TIC	10	3,12
Contra la Constitución	Discriminación a través TIC (art. 510)	141	43,93
Otros		69	1,57
Total		321	100,00

Unidad central criminalidad informática –Fiscalía General del Estado–

Delitos informáticos		Diligencias de investigación	%
Contra la libertad	Amenazas/coacciones a través de TIC (art. 169 y ss y 172 y ss)	2	1,63
Contra la intimidad	Difusión inconsentida de imágenes íntimas (art. 197.7)	1	0,81
De falsedad	Falsificación a través de las TIC	1	0,81
Contra la Constitución	Discriminación a través TIC (art. 510)	118	95,93
Otros	Intrusismo	1	0,81
Total		123	100,00

En el segundo de los cuadros se reseñan las diligencias de investigación incoadas y tramitadas directamente por la Unidad Especializada en Criminalidad Informática a los efectos anteriormente indicados. De entre ellas, 118 tuvieron por objeto la determinación del lugar de comisión/difusión de conductas relacionadas con el discurso del odio *online*, las cuales, una vez realizadas las averiguaciones oportunas para determinar el origen de la publicación, fueron trasladadas a la Unidad contra los Delitos de Odio y Discriminación para su ulterior remisión y tramitación por la fiscalía territorial competente.

Por su parte, las reseñadas en el primero de los cuadros estadísticos, que ascienden a 321, fueron incoadas y tramitadas por las respectivas fiscalías territoriales. El volumen más importante, un 43,93% del total y 141 en números absolutos, es el correspondiente a los delitos de odio y discriminación. También son significativas las cifras referentes a diligencias incoadas por delitos de estafa y/o defraudación, que sumaron 42, poco más del 13% del total, las relativas a actos ilícitos contra la libertad sexual que ascienden en conjunto a 48, casi un 15%, así como las que tuvieron por objeto investigar delitos contra la intimidad, en sus diversas manifestaciones, que alcanzaron la cifra de 39.

En cuanto al estado actual de dichas actuaciones preprocesales en el momento de elaborar esta Memoria, ha de indicarse que el 40,49% de las mismas –130 en números absolutos– fueron remitidas al órgano judicial competente para proseguir la investigación y el 35,20% fueron archivadas al no hallarse indicios suficientes de la comisión de un hecho ilícito. El resto se encuentran actualmente en tramitación por el órgano territorial competente del Ministerio Fiscal.