

8.2 Análisis de las diligencias de investigación y procedimientos judiciales incoados y acusaciones formuladas por el Ministerio Fiscal en 2021

Al igual que en los años precedentes, resulta obligado en esta Memoria reseñar y analizar los datos estadísticos registrados por la Institución en el año 2021 relativos a las investigaciones judiciales o del MF incoadas por ciberdelitos, así como a los escritos de acusación formulados por la Fiscalía en esa materia. Con ello se da cumplimiento a la encomienda reseñada en el artículo 9 del Estatuto Orgánico del Ministerio Fiscal de ofrecer nuestra valoración acerca de *la evolución de la criminalidad, la prevención del delito y las reformas más convenientes para una mayor eficacia de la Justicia*. Es decir, lo que se pretende en este apartado es ofrecer un estudio serio y reflexivo de la incidencia de la cibercriminalidad en sus distintas manifestaciones en el último periodo anual y reflexionar acerca de las variaciones cuantitativas y cualitativas constatadas respecto a otros periodos anuales, así como, sobre las dificultades detectadas en su investigación y persecución penal. Todo ello con el objetivo de promover y facilitar el establecimiento de futuras líneas de actuación, tanto en el ámbito interno de la propia Institución como en lo referente a aspectos legislativos y de carácter estructural u organizativo, que contribuyan a mejorar la eficacia del Estado de Derecho ante un fenómeno criminal extraordinariamente complejo, acusadamente versátil y cuya afectación al interés general y a los derechos de los/as ciudadanos y ciudadanas es cada vez más grave y preocupante.

No obstante, y para garantizar una adecuada interpretación de la información estadística que se ofrece a continuación, es imprescindible recordar que las cifras reseñadas son resultado de la recopilación por parte de esta Unidad especializada de los datos, facilitados por las propias fiscalías territoriales, relativos a las diversas actuaciones jurisdiccionales o del MF correspondientes al año memorial que tuvieron por objeto cualquiera de los delitos competencia del área de especialización tal y como viene delimitada en la Instrucción 2/2011 de la FGE *sobre el Fiscal de Sala de Criminalidad Informática y las secciones de Criminalidad Informática de las Fiscalías*, recientemente actualizada en septiembre del pasado año 2021.

Quiere decirse con ello que estas cifras, y particularmente las referidas a nuevas incoaciones, no tienen por qué coincidir –y de hecho no coincidirán– con la información que anualmente facilita el Ministerio del Interior acerca de la evolución de la cibercriminalidad. En ese sentido, ha de recordarse que los cuerpos policiales, por aplicación de lo

dispuesto en el vigente artículo 284 de la LECrim, no están obligados a trasladar a los órganos judiciales y/o a la Fiscalía aquellos atestados en los que no conste autor conocido ni vías para su posterior determinación, salvo que se trate de alguno de los delitos relacionados en el apartado 1.º del mismo precepto –delitos contra la vida, la integridad física, la libertad o indemnidad sexual o relativos a la corrupción– o cuando así lo interese el MF o la Autoridad Judicial. Lamentablemente, son muchas las investigaciones –particularmente por delitos de estafa o defraudación y también relativas a ataques a sistemas informáticos– en las que, por diversas razones que posteriormente se comentarán, no es posible determinar la autoría y que por tanto ni llegan a conocimiento de los órganos de la jurisdicción penal ni existe constancia de ellas en las aplicaciones informáticas.

También se hace necesario aclarar que, a los efectos estadísticos que nos ocupan, se computan todos los procedimientos por cibercrimitos de los que se ha informado a la Fiscalía, cualquiera que sea su gravedad, es decir, sin distinción en atención a su inicial catalogación como delito grave o leve, dado que se pretende ofrecer una visión lo más próxima posible a la incidencia real que está teniendo el desarrollo tecnológico en las distintas manifestaciones de la delincuencia. Al respecto, no se puede obviar que, en muchas ocasiones, la denuncia inicial de un ilícito *online* aparentemente leve, o que ha causado un perjuicio individual de escasa cuantía, no es sino la toma de conocimiento de una actividad delictiva de mayor envergadura que proyecta sus efectos en distintos territorios, incluso más allá de las propias fronteras del Estado.

Sin olvidar estas precisiones, de la información recabada en los distintos órganos del MF se colige que en el año 2021 se incoaron en España un total de 23.801 procedimientos judiciales y 325 diligencias de investigación del MF por hechos susceptibles de tipificarse en las categorías que nos ocupan, 6.951 más que en 2020 –16.914 y 261 respectivamente–, lo que conlleva un incremento porcentual del 40,47 % en dicho periodo anual.

Este resultado da cuenta igualmente de un claro aumento de la actividad de los órganos de la jurisdicción penal por esta clase de actividades ilícitas, dato que sin duda alguna es indicativo de la progresiva incidencia de este fenómeno criminal. A efectos de corroborar esta afirmación es significativo el análisis de los datos obtenidos en el último quinquenio, comprensivo de los años 2017 a 2021. Seleccionamos este periodo porque 2017 fue la primera anualidad completa en la que se aplicó el nuevo régimen de traslado de atestados previsto en el artículo 284 LECrim, por lo que los presupuestos que determinan la

información remitida a los órganos de la jurisdicción penal sobre investigaciones en curso son homogéneos en dicho periodo temporal. Pues bien, según los datos recogidos en las Memorias de la FGE de dichas anualidades el volumen de actuaciones judiciales por ilícitos de esta naturaleza ha evolucionado desde los 6.676 del año 2017 a los 23.801 del pasado año, dando lugar a un índice de crecimiento de casi el 257 %.

Evidentemente, el incremento interanual ha ido variando en atención a las circunstancias concurrentes en cada periodo. Así, el repunte se concretó en un 35,84 % entre 2017 y 2018 y en casi un 45 % –índice incluso superior al alcanzado en el año memorial– entre 2018 y 2019. Sin embargo, curiosamente, el ritmo de crecimiento acusó una clara ralentización en 2020, anualidad coincidente con la COVID-19, fijándose en un 28,69 %, para incrementarse de nuevo con fuerza en el último periodo anual. Como ya se mencionó en la Memoria del pasado año 2020, aun cuando la actividad delictiva no se redujera en medida alguna durante pandemia, las obligadas medidas de aislamiento, tuvieron una clara repercusión en el traslado de atestados y/o denuncias a los órganos judiciales y a la Fiscalía, así como en el normal desenvolvimiento de la actividad jurisdiccional y también de las indagaciones y averiguaciones policiales sobre hechos ilícitos. Superada la excepcionalidad de esa situación, durante el año 2021, han ido aflorando denuncias e investigaciones pendientes de tramitación, dando lugar a los marcados índices de crecimiento de los que da cuenta esta Memoria.

Esta circunstancia hace imprescindible que desde los poderes públicos se adopten las medidas necesarias para promover y fomentar una mayor y más profunda sensibilización de la ciudadanía acerca de los riesgos que entraña el uso de los instrumentos tecnológicos si no se adoptan las medidas de seguridad exigibles y también para reforzar la capacidad de actuación de los investigadores y operadores jurídicos encargados específicamente de lucha contra este fenómeno criminal, mejorando los medios personales y materiales de los que disponen y proporcionándoles la formación y actualización permanente en las técnicas y habilidades que resultan imprescindibles para la investigación de actividades criminales cuya gravedad y peligrosidad es incuestionable.

El examen de los datos estadísticos sobre procedimientos incoados en el año 2021 ofrece los siguientes resultados:

Delitos informáticos		Procedimientos judiciales incoados	%
Contra la libertad.	Amenazas/coacciones a través de TICs (art. 169 y ss. y 172 y siguientes).	1.890	7,94
	Acoso a través de TICs (art. 172 ter).	490	2,06
Contra la integridad moral.	Trato degradante a través de Tics (art. 173).	102	0,43
Contra la libertad sexual.	Pornografía infantil/ discapaces a través de TICs (art. 189).	777	3,26
	Acosos menores a través de TICs (art. 183 ter).	321	1,35
	Otros delitos c/libertad sexual a través TIC.	412	1,73
Contra la intimidad.	Ataques / interceptación sistemas y datos (art. 197 bis y ter).	97	0,41
	Difusión inconsciente de imágenes íntimas (art. 197.7).	119	0,50
	Descubrimiento/ revelación secretos a través TIC (art. 197).	754	3,17
Contra el honor.	Calumnias/ injurias autoridades a través TIC (arts. 215 y ss.).	182	0,76
Contra el patrimonio y el orden socio-económico.	Estafa cometida a través de las TICs (art. 248 y 249).	17.969	75,50
	Descubrimiento secretos empresa a través de TIC (art. 278 y ss.).	35	0,15
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286).	23	0,10
	Delitos de daños informáticos (arts. 264,264 bis y 264 ter).	125	0,53
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss).	86	0,36
De falsedad.	Falsificación a través de las TICs.	147	0,62
Contra Constitución.	Discriminación a través TIC (art. 510).	221	0,93
Otros.		51	0,21
Total.		23.801	100,00

Del análisis de los datos ofrecidos se constata, al igual que en años anteriores, que los delitos de estafa y/o defraudación de los artículos 248 y ss. CP generaron la incoación de un llamativo número de procedimientos judiciales, que en 2021 se concretó en 17.969 expedientes, el 75,5 % del total de los incoados en ese periodo anual por cualquier clase de ciberdelitos. Su incremento respecto del año 2020 se concreta en 5.719 registros, con un índice al alza del 46,68 % respecto de las cifras obtenidas el año precedente.

Estos resultados, dada la escasa entidad de los índices correspondientes a los restantes ilícitos, podrían llevarnos a considerar que la actividad delictiva en el ciberespacio es en gran medida de contenido económico y de carácter defraudatorio ya que, a excepción de los delitos contra la libertad y seguridad que dieron lugar conjuntamente a algo menos del 10 % de las incoaciones, los relativos a la libertad e indemnidad sexual, que generaron un 6,34 % y los que atentaron contra la intimidad que motivaron el 4 % de esos nuevos registros, la incidencia de los restantes ciberdelitos es inferior al 1 %. Además, esta clara preeminencia de los procedimientos relativos a estafas y defraudaciones frente a los expedientes relativos a otros ilícitos se ha ido incrementando en los últimos periodos anuales pues si en 2018 ofrecía un índice del 61,54 %, dicha cifra se elevó al 65,51 % en 2019 y al 72,43 % en 2020 hasta alcanzar en el pasado año el 75,50 %.

No obstante, y sin negar la gravedad de las conductas fraudulentas *online* y los importantes perjuicios económicos que de ellas se derivan, la valoración adecuada de las cifras que se aportan en este apartado exige hacer determinadas precisiones. Así, en primer término, es un hecho cierto que estas conductas son generalmente objeto de denuncia, por propia decisión de los afectados o incluso, en ocasiones, porque son instados a ello como condición para ser resarcidos de los perjuicios ocasionados. En consecuencia, son comportamientos que habitualmente «aflojan» y llegan a conocimiento de los órganos encargados de la investigación y persecución penal. No ocurre lo mismo con otros tipos de delitos *online*, como los que atentan contra la libertad e indemnidad sexual o algunos otros, como el acoso, las amenazas o los que afectan a la integridad moral, en los que las víctimas o bien no son conscientes de la agresión o bien su propia situación de vulnerabilidad les impide o dificulta la denuncia del hecho criminal. Lo mismo ocurre, aunque por motivaciones diferentes, respecto de otros ilícitos como los ataques a sistemas informáticos. Es por ello que la cifra oculta de criminalidad en algunas otras actividades delictivas es hoy por hoy incalculable y queda al margen de las estadísticas oficiales.

Por otra parte, es conocido que en muchas ocasiones –porque los/ las delincuentes así lo planifican de forma deliberada– una misma acción criminal produce consecuencias en diversos territorios dando lugar de esta forma a un número indeterminado de denuncias que, aunque realmente responden a efectos parciales de esa misma acción ilícita y posteriormente podrían ser acumuladas en un único procedimiento judicial, son respectivamente anotadas en los registros de entrada de múltiples órganos judiciales. Finalmente, otra circunstancia que ha de tenerse en cuenta al analizar las cifras, la categoría correspondiente a las defraudaciones es extraordinariamente abierta y abarca una gran diversidad de comportamientos delictivos que, aun obedeciendo a dinámicas y planteamientos muy diferentes, persiguen el idéntico objetivo de obtener un beneficio en perjuicio de otros a través de una transferencia económica irregular ya sea motivada por engaño, manipulación informática o combinando ambos elementos. Ello explica que acciones criminales muy diversas, cuya investigación y enjuiciamiento plantea problemas diferentes, se cataloguen no obstante de forma conjunta en este apartado, circunstancia que también influye en el abultado resultado expuesto.

Así, dentro del capítulo de las estafas y defraudaciones se incluyen los supuestos en que los/las delincuentes, aprovechando las facilidades de conectividad inherentes a las TIC y su uso habitual en las operaciones comerciales, difunden *online* ofertas fraudulentas de cualquier clase de bienes y servicios, intentando captar la voluntad de terceros que, atraídos por dichas propuestas engañosas, se animan a contratar y a abonar el importe correspondiente viéndose posteriormente perjudicados ya que ni reciben el bien o servicio concertado ni pueden recuperar el desembolso previamente efectuado. Se trata de estafas de corte tradicional, perfectamente encuadrables en el artículo 248-1.º CP, que se han visto favorecidas en su planificación y ejecución por las circunstancias antedichas y cuya incidencia se aprecia en toda clase de actividades mercantiles o comerciales.

Ciertamente, en un principio estas acciones ilícitas respondían a esquemas de actuación muy sencillos, casi artesanales, que se llevaban a efecto a título individual por delincuentes aislados y cuyo esclarecimiento no presentaba mayores dificultades. No obstante, estas actividades se han ido *profesionalizando* con el transcurso del tiempo, a medida que sus responsables, en ocasiones integrados en grupos u organizaciones criminales, se han dotado de habilidades en el uso de los recursos tecnológicos y de conocimientos específicos en las distintas áreas de la actividad económica, comercial o financiera, mejorando de esta forma su capacidad de contactar y convencer a sus

futuras víctimas y también de planificar y desarrollar el *iter criminis*, dando lugar a una actuación criminal más elaborada y compleja que ofrece serias dificultades para su investigación e identificación de sus responsables. En particular, es preocupante la frecuencia con que los/as delincuentes usan falsamente la identidad de otras personas en sus contactos con las futuras víctimas, lo que genera graves consecuencias no solo para la determinación de los responsables criminales sino especialmente para aquellos cuya identidad ha sido falsamente usada, que pueden verse seriamente perjudicados por las acciones realizadas en su nombre.

En los últimos periodos anuales se ha detectado un aumento significativo de causas judiciales que abordan investigaciones por estafas y defraudaciones de estas características, fruto de una planificación cuidadosa y muy elaborada técnicamente, que producen efectos en una gran diversidad de lugares del territorio nacional y en muchas ocasiones más allá de las fronteras nacionales o incluso de otras que, planificadas íntegramente desde el extranjero, tienen como objetivo captar de forma fraudulenta la voluntad de ciudadanos o ciudadanas españoles y de otros países de nuestro entorno más próximo.

Entre ellas van adquiriendo cada vez un mayor protagonismo las que se sirven de la red para publicitar productos financieros que se ofertan engañosamente como inversiones seguras de alta rentabilidad y en condiciones aparentemente muy ventajosas. Quienes planifican estas acciones emplean campañas perfectamente diseñadas, con las que animan a las personas interesadas a efectuar importantes desembolsos económicos confiando erróneamente en conseguir grandes beneficios que nunca llegan a obtener, no logrando tampoco, en muchos de los supuestos, recuperar las cantidades entregadas, dadas las dificultades que plantea incluso la identificación de los delincuentes o la determinación del país desde el que están actuando.

También es cada vez más habitual que quienes cometen estas defraudaciones soliciten o sugieran a los/as inversores que su aportación se realice en activos digitales o más concretamente en criptomonedas, lo que está determinando que un número cada vez mayor de ciudadanos/as, convencidos de la bondad de la propuesta, inviertan en dichas operaciones ingentes cantidades de dinero que los/as delincuentes aprovechan en propio beneficio. De hecho, es significativo el volumen de causas judiciales en tramitación por supuestas operaciones económicas en las que se emplean fraudulentamente como reclamo las ventajas que presuntamente ofrecen estos criptovalores, dado el carácter anónimo de las transacciones y la posibilidad que brindan de obtener rápidas ganancias.

En estos casos a las dificultades inherentes a este tipo de investigaciones se añaden las derivadas de la intervención, en muchos de los supuestos, de proveedores de servicios de intermediación y cambio de monedas virtuales y de custodia de monederos electrónicos radicados frecuentemente en el extranjero, lo que complica significativamente la trazabilidad de los movimientos económicos realizados. No obstante, esta última circunstancia va a poder solventarse, al menos parcialmente, tras la reciente publicación del Real Decreto Ley 7/2021 de 7 de abril, que incorpora al ordenamiento interno la Directiva (UE) 2018/843 *sobre prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo* y atribuye a estas entidades de intermediación la cualidad de sujetos obligados a esos efectos, por lo que quedan sometidos al deber de inscribirse en el Registro creado a dicho fin en el Banco de España y también a informar acerca de aspectos tales como las operaciones económicas que hayan gestionado, los ordenantes y destinatarios de las mismas o los titulares de los correspondientes monederos electrónicos, medidas que contribuirán, sin duda, a facilitar la investigación de las conductas que nos ocupan.

Sin perjuicio de ello, conscientes de las dificultades para hacer frente a estas formas de defraudación y también de la importancia de fijar, en el seno de la Institución, criterios de actuación que permitan solventar las múltiples cuestiones jurídicas y técnicas que se plantean en la fase de instrucción y enjuiciamiento de estas conductas, una de las conclusiones adoptadas en las últimas Jornadas de Especialistas del pasado mes de noviembre fue, precisamente, la de encomendar a la Unidad especializada el seguimiento pormenorizado de las diversas causas judiciales en curso por ilícitos de esta naturaleza y la toma de contacto con los restantes organismos implicados en esta problemática –tales como la CNMV, la ORGA o el Banco de España– con el objetivo de elaborar un protocolo de actuación que haga posible mejorar la capacidad de respuesta ante estas criminales conductas.

Estas nuevas manifestaciones de la estafa tradicional, basada en el engaño de la víctima, coexisten con otras formas de defraudación que se sirven de la manipulación informática para dar lugar al desplazamiento patrimonial no consentido y también con otras supercherías que combinan ambos elementos para hacer posible la transferencia económica en provecho de los propios responsables criminales o de sus beneficiarios. Del primer grupo es un claro exponente la técnica del *pharming*, que consiste en redirigir la dirección web solicitada por el/la internauta a un sitio web falso controlado por el agresor que imita fraudulentamente aquél al que se pretende acceder –normalmente el

correspondiente a una entidad bancaria– para apoderarse de esta forma de las claves y contraseñas del perjudicado/a o de cualquier otra información de interés. En estos casos la víctima no se ve abocada a un proceso mental erróneo, basado en un engaño previo, sino que la captación de sus claves se produce como consecuencia de la alteración producida en el funcionamiento del sistema mediante técnicas de ingeniería informática.

No obstante, las conductas más frecuentes en la práctica, y las que determinan la incoación del mayor volumen de causas judiciales, son las que combinan en diversas formas ambos elementos: engaño y manipulación informática. Sin pretensión de exhaustividad, dadas las limitaciones de espacio, citamos a modo de ejemplo los ataques de *Business Email Compromise* (BEC), que afectan generalmente a entidades empresariales y en los que los/las delincuentes, tras obtener por medios diversos información sobre el funcionamiento interno de la empresa atacada, sus responsables y las operaciones comerciales en curso, suplantando la identidad de quienes gestionan el tráfico ordinario de la entidad, o de alguno de sus clientes o proveedores, y ordenan falsamente en su nombre operaciones económicas *online*, aparentemente justificadas, desviando de esta forma importantes cantidades de dinero en su propio beneficio. E igualmente son objeto de investigación en diversas causas judiciales supuestos de la llamada *estafa del soporte técnico*, actividad en la que los/las agresores/as, tras infectar el dispositivo de la víctima mediante una intrusión irregular, simulan un mal funcionamiento del sistema para posteriormente justificar el ofrecimiento al afectado/a de la posibilidad de contactar telemáticamente con el correspondiente equipo técnico para su subsanación. Esto les permite, haciéndose pasar por encargados de la reparación, tomar el control del sistema y llevar a efecto sus criminales objetivos, ya sea exfiltrar información, obtener datos personales de la víctima o simplemente cobrar reparaciones no realizadas.

Otra forma de defraudación de especial interés, que ha determinado la tramitación en el año memorial de varios procedimientos judiciales es la denominada *SIM Swapping*. El objetivo de los delincuentes es sortear las medidas establecidas para garantizar la seguridad de las operaciones bancarias *online*. Con esa finalidad logran hacerse, por distintos medios, con duplicados de las tarjetas SIM de los/las titulares de las cuentas bancarias contra las que pretenden operar, lo que les permite conocer los códigos de confirmación de las transacciones electrónicas que se comunican a los/as clientes a través de mensajes SMS y, por ende, autorizar directamente las operaciones que ellos

mismos han ordenado en su propio beneficio, sin conocimiento alguno por parte de las víctimas.

Sin embargo, el mayor volumen de denuncias y/o investigaciones encuadrables en este apartado sigue correspondiendo a los casos de utilización irregular *online* de numeraciones de tarjetas ajenas de crédito o débito, previamente obtenidas mediante técnicas de *skimming*, *phishing* o *hacking*, entre otras, que, según información policial, suponen aproximadamente, el 70 % de las denuncias por defraudación *online*. Buena parte de las investigaciones por hechos de esta naturaleza ni tan siquiera llegan a conocimiento de los órganos de la jurisdicción penal, por mor de lo dispuesto en el artículo 284 LECrim, dadas las dificultades técnicas y jurídicas para la determinación de sus autores que, en muchas ocasiones, operan desde otros países.

Un capítulo importante en la Memoria de Criminalidad informática es, sin duda, el dedicado a las agresiones contra bienes de carácter personalísimo de entre las cuales destacan por su mayor incidencia –que en 2021 se aproxima al 10 % del total de procedimientos por ciberdelitos– aquellas que afectan a la libertad y seguridad de las personas. En el año 2021 estos delitos dieron lugar a la incoación de 2.380 expedientes judiciales, 670 más que en 2020, con un índice conjunto de crecimiento del 34,50 % respecto del año anterior. No obstante, estos ilícitos, que agrupamos a estos efectos en dos grandes apartados –el relativo a las amenazas y coacciones en el entorno tecnológico y el del acoso permanente u hostigamiento, conocido como *stalking*, del artículo 172 ter CP– presentan marcadas diferencias en su evolución estadística ya que el significativo incremento interanual del primero de ellos, cifrado en más de un 51 % contrasta con la progresión más moderada del segundo, con un 5,8 %. Los procedimientos incoados en 2021 por esta figura del *stalking* confirman una tendencia a la estabilidad, ya detectada en 2020, tras el marcado índice de crecimiento –superior al 100 %– en el volumen de incoaciones registrado en este apartado entre los años 2017 y 2019. En cualquier caso, hemos de precisar que las anotaciones por delitos del artículo 172 ter CP se refieren, en términos generales, a causas seguidas por hechos incardinables con carácter exclusivo en dicho precepto ya que si concurren con delitos de amenazas o coacciones la anotación normalmente se efectúa en el apartado correspondiente a estos últimos dada su mayor gravedad.

Estos comportamientos, en múltiples ocasiones, aparecen vinculados al ámbito de la violencia de género y, por ello, son objeto también de seguimiento en el área de especialización encargada específicamente de dicha materia, pero igualmente se detectan con frecuencia respecto de personas con las que él o la atacante mantiene cualquier otro tipo de

relación, ya sea laboral, de amistad o fruto de encuentros esporádicos e incluso, en ocasiones, respecto de personas desconocidas para el/la agresor/a en cuyo caso la selección de la víctima se efectúa de forma aleatoria. Tal es el caso de las denuncias por *sextorsión*, en las que, en ocasiones el/la delincuente ni tan siquiera tiene un su poder imágenes comprometidas de la víctima, sino que se limita a hacerle creer que dispone de ellas o conoce de contactos o intentos de contacto que le pueden comprometer. Aunque son supuestos en los que difícilmente se llega a identificar a sus responsables, generan un volumen considerable de denuncias que tienen su reflejo en los datos expuestos.

Merecen consideración especial, por su afectación a bienes personales de singular relevancia, los expedientes por delitos contra la libertad e indemnidad sexual. El número total de los incoados en el año asciende a 1.510, cifra que da cuenta de un incremento del 5,44 % respecto de los 1.432 registrados, en esta categoría, en la anualidad precedente. Los más numerosos son los relativos a delitos de pornografía infantil y/o de personas con discapacidad que sumaron 777 registros, 70 más que en 2020, lo que implica un índice de crecimiento del 9,90 % que, si bien ha de considerarse moderado, es reflejo de un significativo cambio en la tendencia descendente que veníamos observando desde el año 2018. Como ya se ha mencionado, todos los indicativos nacionales e internacionales dan cuenta de un progresivo aumento en el tráfico online de material de abuso infantil por lo que estos resultados, aunque discretos, apuntan a una mayor capacidad de respuesta de cuerpos policiales y de los órganos jurisdiccionales ante este gravísimo fenómeno criminal.

También evolucionan al alza, con un índice de crecimiento del 7,85 % los procedimientos por otros tipos delictivos contra la libertad e indemnidad sexual –exhibicionismo, abuso y agresión sexual online, provocación sexual, etc.– con la única excepción de los delitos de *child grooming* en los que se detecta un descenso, cifrado en 28 expedientes, respecto de los 349 registrados en 2020. Esta puntual reducción en el número de procedimientos por este delito previsto en el artículo 183 ter CP, cuyo progresivo incremento venía siendo una constante en periodos anuales precedentes, puede estar motivada por la concurrencia, en muchos supuestos, de la conducta sancionada en el apartado segundo de dicho precepto con la de elaboración de material pornográfico infantil del art. 1891.º a) CP, lo que determina que el *child grooming*, por aplicación de las reglas del concurso de normas, quede absorbido por esta última figura.

Por su parte, las causas judiciales por actos que atentan *online* contra la intimidad, los datos personales o la inviolabilidad de las

comunicaciones, aumentaron en conjunto en un 28,47 % respecto de los registros obtenidos en 2020. La comparativa parcial entre los distintos tipos penales que encuadramos en este apartado se oscurece ligeramente porque en esta ocasión, por primera vez, ofrece registros independientes sobre la conducta de difusión no autorizada de imágenes íntimas del artículo 197.7 CP que, en consecuencia, no son susceptibles de contraste con los de años anteriores y que, además, han de tomarse con especial cautela dado que algunas Fiscalías provinciales carecen por el momento de información individualizada en relación con ello. No obstante, es interesante reseñar que el crecimiento anual, cifrado en conjunto en 215 expedientes, se integra por los 119 incoados en base al artículo 197.7 y las 59 y 37 anotaciones en que se concreta, en el primer caso, el aumento de las conductas encuadrables en los restantes apartados del artículo 197 y, en el segundo, en las relativas a los artículos 197 bis 1.º y 2.º y 197 ter que tipifican actos relacionados con ataques a los sistemas de información.

Al reflexionar sobre estos delitos llama la atención el número creciente de procedimientos por conductas en las que el atentado contra estos derechos fundamentales se realiza por medios tecnológicos. El almacenamiento generalizado de información reservada o de carácter personal en dispositivos, sistemas informáticos o bases de datos, determina que el acceso no autorizado a dicha información se lleve a efecto, generalmente, a través de dichos medios lo que en consecuencia hace que los órganos de la jurisdicción penal hayan de pronunciarse sobre una gran diversidad de acciones de estas características. Esta circunstancia está dando lugar a una variada e interesante doctrina jurisprudencial, en referencia particularmente a los artículos 197-1.º y 2.º, que resulta de especial utilidad en la interpretación de estos tipos penales.

Los procedimientos por delitos de ataques a sistemas informáticos sancionados en los artículos 197 bis y ter CP tuvieron en 2021 un repunte del 61,66 %, índice considerablemente más alto que el detectado respecto de los delitos de daños informáticos que se fija en un 26,26 %, al aumentar el volumen de expedientes desde los 99 incoados en 2020 a los 125 del año memorial. En conjunto se ha registrado un crecimiento de casi un 45 % en las causas judiciales relativas a estas agresiones informáticas, algunas de las cuales tienen por objeto la investigación de ataques de *ransomware* especialmente relevantes por la naturaleza y funciones de los organismos que se vieron afectados. Por ello, y aunque estos resultados siguen siendo muy reducidos a tenor del número de agresiones contra sistemas de información e incidentes de seguridad registrados anualmente por las entidades responsables de la seguridad en el ciberespacio, el dato ofrecido es espe-

ranzador y da cuenta de la creciente concienciación de la sociedad sobre la importancia de promover la respuesta penal frente a estas agresiones y también de los positivos efectos de la puesta en funcionamiento del sistema establecido por los Reales Decretos 12/2018 y 43/2021 sobre seguridad de redes y sistemas de información para trasladar al MF y a la Policía Judicial las notificaciones que presenten caracteres de delito.

Se cierra este análisis sobre los procedimientos judiciales incoados en 2021 con una breve referencia al destacadísimo incremento en el volumen de los que tuvieron por objeto la investigación de delitos de odio *online*, que ascienden a la cifra de 221, frente a los 80 del año 2020, con un índice al alza de más de un 175 %. Este excelente resultado es el mejor indicativo del esfuerzo del MF en la lucha contra estas gravísimas conductas que atentan no solo contra los derechos e intereses de los afectados sino también contra los principios y valores en que se sustenta el Estado de Derecho. El trabajo desarrollado conjuntamente por quienes integran sendas áreas ha hecho igualmente posible, en el año memorial, la puesta en funcionamiento del *Protocolo para la retirada de la red de contenidos relacionados con el discurso de odio*, al que nos referimos detalladamente en otro apartado de esta misma Memoria.

8.2.1 ESCRITOS DE ACUSACIÓN DEL MINISTERIO FISCAL

Los datos derivados de los escritos de acusación, al igual que los relativos a las Diligencias de Investigación del MF, adquieren un especial interés en el estudio sobre la evolución de la ciberdelincuencia en el año memorial que nos ocupa, dado que se trata de información mucho más precisa y depurada que la obtenida a partir de los registros de incoación de procedimientos judiciales. Ciertamente, esta última permite vislumbrar de una forma más completa el conjunto de denuncias y/o atestados policiales que han llegado a conocimiento de los órganos judiciales en los distintos territorios del Estado por lo que su valor, desde el punto de vista cuantitativo, es indiscutible. No obstante, la calidad de dicha información en referencia a las diferentes tipologías delictivas se encuentra profundamente condicionada por las limitaciones derivadas del momento en que se efectúa el registro, al inicio mismo de la investigación, cuando todavía no se ha definido claramente el contenido y alcance real de la infracción criminal.

Por el contrario, los datos que se examinan a continuación se refieren a actuaciones realizadas por la propia Fiscalía y, concretamente se

incluyen en este apartado los escritos de acusación elaborados por el MF, una vez finalizada la investigación criminal, a partir del estudio detallado y pormenorizado de los hechos probados y de su valoración técnico jurídica con arreglo a criterios de legalidad e imparcialidad por lo que la trascendencia de la información que de ellos se deriva resulta, sin duda alguna, incuestionable. Sin perjuicio de ello, es importante aclarar que los datos que se examinan a continuación adolecen de algunas carencias dado que, por deficiencias en el registro informático, en los numerosos supuestos en que la acusación se formula por una pluralidad de ilícitos, de igual o diferente naturaleza, por lo general solo se deja constancia estadística del más significativo de los mismos, desechándose la información sobre los restantes. En consecuencia, los datos con los que se cuenta se refieren al número de escritos de acusación presentados y a la figura delictiva principal o más grave que fue objeto de imputación en cada caso, por lo que, sin negar su valor, no constituyen un reflejo fiel del volumen total de conductas ilícitas –ni de las categorías típicas a las que pertenecen– que fueron objeto de acusación por el Ministerio Fiscal en el año 2021.

A tenor de la información facilitada por los órganos provinciales, el número de escritos de acusación presentados por la Institución en el año 2021, en referencia a ciberdelitos incluidos en el marco de la Instrucción FGE 2/2011 antes citada, fue de 4.104, 897 más que en el año 2020, lo que da cuenta de un incremento porcentual del 27,97%. El crecimiento progresivo, aun con ligeros altibajos, en los datos correspondientes a los escritos de acusación formulados por el MF en esta materia en los últimos años –que reseñamos a continuación– constituyen un buen indicativo de la expansión de este fenómeno criminal y de la respuesta que se está dando al mismo desde el Estado de Derecho.

Año	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Acusaciones.	906	1092	1262	1275	1242	1648	1715	1955	2847	3207	4104

Como puede observarse, en el año memorial se ha producido un claro repunte en el número de acusaciones, notablemente superior al 12,64% registrado en el periodo interanual 2019-2020, como consecuencia muy probablemente de la *normalización* en la actividad ordinaria de los órganos de la jurisdicción penal, una vez superadas las circunstancias excepcionales generadas por la pandemia que provocaron una cierta ralentización en la tramitación de los procedimientos judiciales. Se recupera de esta forma el ritmo de constante crecimiento que venimos observando en los últimos años, solo inte-

rrumpido muy levemente entre los años 2014 y 2015 en el que detectamos un descenso del 2,5 %.

Los datos parciales en función de las tipologías delictivas son los siguientes:

Delitos informáticos		Calificaciones	%
Contra la libertad.	Amenazas/coacciones a través de TICs (art. 169 y ss. y 172 y ss.).	419	10,21
	Acoso a través de TICs (art. 172 ter).	175	4,26
Contra la integridad moral.	Trato degradante a través de Tics (art. 173).	21	0,51
Contra la libertad sexual.	Pornografía infantil/discapaces a través de TICs (art. 189).	368	8,97
	Acosos menores a través de TICs (art. 183 ter).	114	2,78
	Otros delitos c/libertad sexual a través Tic.	110	2,68
Contra la intimidad.	Ataques / interceptación sistemas y datos (art. 197 bis y ter).	9	0,22
	Difusión in consentida de imágenes íntimas (art. 197.7).	32	0,78
	Descubrimiento / revelación secretos a través TIC (art. 197).	208	5,07
Contra el honor.	Calumnias / injurias autoridades a través TIC (art. 215).	21	0,51
Contra el patrimonio y el orden socio-económico.	Estafa cometida a través de las TICs (art. 248 y 249).	2282	55,60
	Descubrimiento secretos empresa a través de TIC (art. 278 y ss.).	10	0,24
	Delitos c/ servicios de radiodifusión / interactivos (art. 286).	68	1,66
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter).	18	0,44
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss.).	81	1,97

Delitos informáticos		Calificaciones	%
De falsedad.	Falsificación a través de las TICs.	56	1,36
Contra Constitución.	Discriminación a través TIC (art. 510).	70	1,71
Otros.		42	1,02
Total.		4.104	100,00

Siguiendo la tónica de años anteriores, el número más elevado de escritos de acusación corresponde a las estafas y defraudaciones, que sumaron 2.282, el 55,6 % del total de los formulados por la Fiscalía, seguido por los correspondientes a los delitos contra la libertad y seguridad de las personas –amenazas, coacciones y acoso permanente– que dieron lugar conjuntamente a 594 escritos de conclusiones provisionales, un 14,47 % del total de los elaborados en el año. En relación con las primeras se constata un incremento porcentual de casi el 60 % respecto de las 1.463 calificaciones efectuadas por estafa o defraudación en 2020. Sin embargo, ese crecimiento interanual es mucho más moderado en referencia a los delitos contra la libertad y seguridad, al rebasar levemente el 10 %.

Por su parte, los delitos contra la libertad e indemnidad sexual, en sus distintas manifestaciones, determinaron la presentación de 592 escritos de acusación, 81 más que en el año anterior, repunte que se concreta casi íntegramente en las conductas relacionadas con la elaboración y/o distribución de pornografía infantil o de personas con discapacidad, que suman en el año memorial 80 escritos más que en 2020, con un índice de crecimiento interanual del 27,7 %.

Estas diferencias han de relacionarse con el propio ritmo de evolución del volumen de expedientes incoados por las respectivas tipologías delictivas, aunque el análisis comparativo de uno u otro dato ha de hacerse con especial cautela ya que en un número de supuestos indeterminado –y probablemente elevado– la presentación del escrito de acusación no se efectúa en la misma anualidad de inicio del procedimiento. Sin perder de vista esa precisión, es significativo que el porcentaje de acusaciones presentadas por estafa sea inferior al 13 % en comparación con el número de procedimientos incoados en el año por esa misma categoría delictiva, en tanto que el que se obtiene, fruto de similar contraste, respecto de los delitos contra la libertad y seguridad de las personas se aproxima al 25 % y el correspondiente a los delitos de pornografía infantil supera el 47 %.

Con las salvedades antes indicadas, estos resultados obedecen a la diversa problemática que plantea la actuación frente a las diversas manifestaciones de la delincuencia *online*. Así, por ejemplo, las conductas fraudulentas son habitualmente objeto de denuncia y, por ende, del correspondiente registro, aunque las dificultades que se generan posteriormente en su investigación y en la determinación de sus autores hacen que en muchos supuestos no sea posible concretar la acusación. Por contra en las actividades relacionadas con la pornografía infantil la mayor dificultad estriba en la especial opacidad de estos comportamientos y en la inexistencia de denuncias, pero, una vez los cuerpos policiales o los órganos de la jurisdicción penal detectan –ya sea por propia actuación o por indicación de cuerpos policiales de otros Estados u organismos internacionales– las direcciones IP desde las que se está difundiendo o compartiendo dicho material, a los efectos de formular acusación, la investigación puede orientarse de forma eficaz contra personas concretas, lo que explica que el índice de eficacia sea bastante superior. No obstante, hemos de recordar que las nuevas técnicas de distribución de pornografía infantil a través de archivos compartidos en la *nube* o de aplicaciones de mensajería instantánea están dificultando también de forma importante, en los últimos años, estas indagaciones.

En 2021, los atentados contra la intimidad generaron 249 escritos de acusación, un 6 % del total de los presentados por la Fiscalía, de los que 32 se formularon por el delito sancionado en el art. 197.7 y 208 por cualquiera otra de las conductas sancionadas en los restantes apartados del mismo precepto, lo que da cuenta, por tanto, de un incremento del 16,35 % respecto de los datos obtenidos en la anualidad precedente por esos mismos conceptos.

Finalmente hay que mencionar la marcada evolución al alza de las acusaciones por delitos de odio y/o discriminación, que ascienden a 42 en el año memorial con un índice de crecimiento de más de 300 % respecto de los 8 escritos formulados en 2020 en esta materia. Estos datos son el resultado del esfuerzo empeñado, por los cuerpos policiales, el MF y los órganos judiciales, en la lucha contra esas graves manifestaciones criminales.

8.2.2 DILIGENCIAS DE INVESTIGACIÓN DEL MINISTERIO FISCAL

Como se apuntó anteriormente, pese al reducido número de estos expedientes el valor de la información que generan no es en absoluto desdeñable, ya que, al incoarse y tramitarse en las propias Fiscalías, es

posible un control pormenorizado de su evolución y un conocimiento detallado de la información que de ellas se deriva.

Se trata, como es sabido, de actuaciones de naturaleza preprocesal, dirigidas directamente por el MF, que pueden incoarse de oficio o por denuncia de terceros y que tienen su soporte legal en los artículos 773-2.º de la LECrim y 5 de nuestro Estatuto Orgánico. La tramitación de dichas diligencias se encuentra limitada tanto temporalmente, por el artículo 5 del propio Estatuto Orgánico, como por la previsión del párrafo último del citado artículo 773-2.º, que impone la remisión de lo actuado al órgano judicial competente cuanto se constate la tramitación de procedimiento penal por los mismos hechos que investiga la Fiscalía. Además, la exigencia constitucional y legal de autorización judicial para llevar a efecto la mayoría de las actuaciones que inciden en derechos fundamentales, determina igualmente la necesidad de remitir las diligencias a los órganos judiciales tan pronto como sea necesaria la práctica de las mismas para la prosecución de la investigación.

El número de diligencias de esta naturaleza incoadas el pasado año por los diversos órganos del MF ascendió a 333, cuyo detalle se especifica en la tabla que insertamos a continuación:

Delitos informáticos		Diligencias de investigación	%
Contra la libertad.	Amenazas/coacciones a través de TICs (art. 169 y ss. y 172 y ss.).	7	2,1
	Acoso a través de TICs (art 172 ter).	3	0,9
Contra la integridad moral.	Trato degradante a través de TICs (art 173).	1	0,3
Contra la libertad sexual.	Pornografía infantil/discapaces a través de TICs (art. 189).	7	2,1
	Acoso menores a través de TICs (art. 183 ter).	2	0,60
	Otros delitos c/libertad sexual a través Tic.	11	3,3
Contra la intimidad.	Ataques / interceptación sistemas y datos (art. 197 bis y ter).	2	0,6
	Difusión in consentida de imágenes íntimas (art. 197.7).	3	0,9
	Descubrimiento/ revelación secretos a través TIC (art 197).	23	6,91

Delitos informáticos		Diligencias de investigación	%
Contra el honor.	Calumnias/ injurias autoridades a través TIC (arts. 215 y ss.).	10	3
Contra el patrimonio y el orden socio-económico.	Estafa cometida a través de las TICs (art. 248 y 249).	181	54,35
	Descubrimiento secretos empresa a través de TIC (art. 278 y ss.).	1	0,3
	Delitos c/ servicios de radiodifusión / interactivos (art. 286).	1	0,3
	Delitos de daños informáticos (arts. 264,264 bis y 264 ter).	5	1,5
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss.).	4	1,2
De falsedad.	Falsificación a través de las TICs.	2	0,6
Contra Constitución.	Discriminación a través TIC (art. 510).	69	20,72
Otros.		1	0,3
Total.		333	100

Las limitaciones antedichas determinan que el margen de utilización de estos expedientes en materia de ciberdelincuencia sea muy reducido ya que, en muchos casos, las diligencias necesarias para el esclarecimiento de conductas cometidas a través de los medios y sistemas informáticos precisan de la mencionada autorización judicial por afectar a información incluida dentro de lo que se ha venido a llamar el derecho fundamental a la intimidad en el entorno virtual. Pese a ello, el número de diligencias de investigación que se incoan y tramitan en la Fiscalía sigue aumentando año a año para responder a las demandas de los ciudadanos y de los organismos e instituciones que trasladan sus denuncias a la Institución, circunstancia que se corrobora con los datos que ofrecemos indicativos del crecimiento en más de un 27 % respecto de los 261 expedientes de esta naturaleza incoados en 2020.

La cifra más elevada, en coherencia con los resultados obtenidos en otros ámbitos, corresponde a las estafas y defraudaciones, conductas cuya investigación dio lugar a la incoación de 181 diligencias, 85 más que en 2020, que suponen más de un 54 % del total de las registradas en el año. Le siguen en importancia las diligencias relativas a

delitos de odio y discriminación cometidos a través de la red, que determinaron la incoación de 69 expedientes, cifra exactamente igual a la obtenida por este concepto en 2020. En este apartado hemos de mencionar igualmente las 70 diligencias incoadas en el año memorial por esta Unidad especializada, que no computamos estadísticamente ya que nuestra intervención se limitó a la determinación, al amparo de lo dispuesto en la Circular 4/2013 FGE, del órgano del MF territorialmente competente para el conocimiento de los hechos. Con un volumen muy inferior, destacan en el año 2021 los 28 expedientes por delitos contra la intimidad y los 20 que tuvieron por objeto presuntos atentados contra la libertad e indemnidad sexual.

Del conjunto de las diligencias de investigación incoadas un 43,54 % fueron remitidas a los órganos judiciales competentes para proseguir la investigación ya fuera por haber constatado la existencia de proceso judicial previo, por precisar la práctica de diligencias de investigación reservadas a la autoridad judicial o por haberse obtenido indicios suficientes de la comisión de actividades delictivas. Por su parte, 136 fueron archivadas y el resto continuaban en tramitación al iniciarse el año 2022.