8.2 **Análisis de las diligencias de investigación y procedimientos judiciales incoados y acusaciones formuladas por el Ministerio Fiscal en 2022**

Este apartado de la Memoria tiene como objetivo reseñar y analizar los datos estadísticos registrados por la Institución en el año 2022 sobre investigaciones judiciales o del Ministerio Fiscal incoadas en dicho periodo y también los relativos a escritos de acusación formulados por las y los fiscales por actividades delictivas que, en atención a su naturaleza, a los bienes jurídicos afectados o a la forma o medios en que se lleva a efecto su planificación y ejecución, son susceptibles de encuadrarse en el concepto de ciberdelincuencia que se define en la Instrucción 2/2011 de la Fiscalía General del Estado sobre *el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías*. Con ello se da cumplimiento a la encomienda que nos hace el art. 9 de nuestro Estatuto Orgánico 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.*

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 anteriores periodos anuales, sobre las nuevas manifestaciones criminales o formas de comisión detectadas y también sobre las dificultades que estamos encontrando en la investigación y persecución de estas conductas, tanto en aspectos relacionados con el esclarecimiento de los hechos e identificación de sus autores, como en lo relativo a las herramientas legales disponibles para actuar penalmente frente a estas versátiles conductas. Todo ello con el objetivo no solo de informar a la sociedad sobre la evolución de este fenómeno criminal y de la actuación de la fiscalía ante el mismo, sino también de promover y facilitar la toma de decisiones ya sean legislativas, estructurales u organizativas acerca de las medidas más convenientes para mejorar la eficacia del Estado de Derecho ante esta forma de delincuencia.

Es importante dejar constancia de que los datos con los que contamos provienen de información facilitada por los órganos territoriales del Ministerio Fiscal a partir de las propias actuaciones de quienes integran la Institución, de nuestra intervención directa en los procedimientos tramitados por los órganos judiciales y del seguimiento de la actividad investigadora desarrollada por los cuerpos policiales nacionales y autonómicos respecto de actividades delictivas que, por sus carac-

terísticas y/o por su planificación y ejecución en el entorno virtual, encuadramos en el marco de actuación de este área de especialización.

Se trata, por tanto, de una información que puede no corresponderse exactamente con los datos registrados por los órganos judiciales, porque es más que probable que un número indeterminado de procedimientos incoados no hayan llegado a ser trasladados a las fiscalías en el mismo periodo anual. Tampoco con la información que facilita al respecto el Ministerio del Interior, ya que, por mor de lo dispuesto en el art. 284 LECrim, una buena parte de las investigaciones iniciadas por los cuerpos policiales no son remitidas a las autoridades judiciales ni a las fiscalías al no estar identificado el autor de los hechos ni existir líneas de investigación para averiguarlo. Por otra parte, las limitaciones y carencias de nuestras aplicaciones informáticas pueden determinar también inexactitudes o deficiencias en el registro de expedientes o en la identificación jurídica de los ilícitos que han motivado su incoación, lo que genera desviaciones respecto de las situaciones realmente producidas.

Hechas estas aclaraciones, necesarias para la correcta valoración de los datos que ofrecemos, ha de ponerse en valor la información obtenida pues, al margen de tales limitaciones, su recopilación año a año de forma sistemática y a partir del seguimiento directo por parte de los/as fiscales de las actuaciones que las sustentan hacen de ella un indicador de especial interés a efectos de valorar no solo la incidencia de la ciberdelincuencia sino también las futuras tendencias en la planificación y ejecución de actuaciones delictivas en la red y, por ende, sirven de base para conocer las necesidades que han de abordarse para proteger a los/as ciudadanos/as frente a estas graves conductas.

Según la información recopilada en el pasado año 2022 se incoaron en España un total de 24.622 procedimientos judiciales y 218 diligencias de investigación de las fiscalías por actividades ilícitas incluidas en el concepto de ciberdelincuencia, tal y como se define en la Instrucción 2/2011 FGE, lo que supone un total de 24.840 expedientes que comparados con los 24.126 incoados en 2021 (23.801 procedimientos judiciales y 325 diligencias de investigación) suponen un ligero incremento de casi un 3% en el último periodo anual. Si bien este porcentaje es moderado en comparación con el de más de un 40% detectado en el periodo interanual 2020-2021, supone la consolidación de la tendencia al alza en el volumen de investigaciones penales por ciberdelitos de la que venimos dando cuenta en anteriores Memorias, y en la que, sin duda, está influyendo la profunda y constante digitalización de las relaciones interpersonales y de la actividad social en su conjunto.

Dicha progresión se constata claramente a partir de algunos de los datos que entresacamos de la información publicada en anteriores Memorias. A dicho fin, resulta de interés tomar como referencia los resultados obtenidos por este mismo concepto en periodos anuales precedentes especialmente significados por motivos diversos, como las 13.143 causas por ciberdelitos registrados en 2019, año inmediatamente anterior a la pandemia, o los 6.676 del año 2017, primera anualidad en la que se consolidó el nuevo régimen de traslado de atestados establecido en el art. 284 LECrim, sentándose las bases de los parámetros actualmente vigentes. Comparando dichos datos con los del año memorial el porcentaje de aumento se sitúa en poco más del 87% en referencia a 2019 y en casi un 269% respecto de 2017, habiéndose mantenido constante desde entonces dicha tendencia alcista.

Sin perjuicio de las notables diferencias entre estas cifras y las ofrecidas por el Ministerio del Interior en el informe publicado en marzo del presente año, que se justifican en buen medida –como ya se ha explicado– porque únicamente se trasladan a la autoridad judicial y a la fiscalía las diligencias relativas a investigaciones en las que es posible la determinación del autor o concurren algunas otras circunstancias específicas, los resultados de una y otra Institución no solo son coincidentes en la constatación de ese incremento constante y significativamente acelerado de la actividad delictiva en la red, sino incluso bastante aproximados en el ritmo de evolución de este fenómeno criminal en los periodos indicados. No en vano el citado informe deja constancia de un aumento de un 22,9 % en el número de investigaciones policiales por cibercrimen iniciadas en el año 2022 respecto de las registradas en 2021, índice que se eleva a un 72% en comparación con los registros del año 2019 y alcanza una cifra muy próxima al 220% respecto del volumen de investigaciones iniciadas en 2017.

Esta clara progresión cuantitativa va acompañada del advenimiento de inéditas formas de lesión de bienes jurídicos necesitados de protección penal. Lo estamos percibiendo en acciones *online* contra bienes personalísimos como la intimidad o la libertad y seguridad, hasta el punto de haber dado lugar a la tipificación de novedosas figuras delictivas que hagan factible la persecución penal de dichas conductas, o también en las agresiones sexuales a menores de edad en el entorno virtual; en las nuevas formas de defraudación y uso fraudulento de instrumentos de pago distintos del efectivo materiales o inmateriales y en los ataques a la seguridad de redes o sistemas informáticos. Sin olvidar tampoco las diversas y variadas formas de utilizar estas tecnologías para la difusión de contenidos capaces de poner en riesgo los valores esenciales de nuestro sistema jurídico y de nuestro modelo

de convivencia que, concurriendo determinados requisitos, pueden también integrar conductas delictivas. En todo caso es incuestionable que el desarrollo tecnológico nos enfrenta a una realidad criminológica abierta y versátil que alcanza a todo tipo de manifestaciones delictivas y que para su abordaje exige de un especial esfuerzo no solo de los operadores jurídicos y de los investigadores sino también del poder legislativo y de la sociedad en su conjunto.

Los datos estadísticos anteriormente indicados en relación con los procedimientos judiciales registrados en el año 2022 se concretan, según la información de la que dispone el Ministerio Fiscal, en las siguientes categorías:

Delitos informáticos		Procedimientos judiciales incoados	%
Contra la libertad	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss.)	1.248	5,07
	Acoso a través de TICs (art. 172 ter)	472	1,92
Contra la integridad moral	Trato degradante a través de TICs (art. 173)	178	0,72
Contra la libertad sexual	Pornografía infantil/ discapaces a través de TICs (art. 189)	832	3,38
	Acosos menores a través de TICs (art 183 ter)	183	0,74
	Otros delitos c/libertad sexual a través TIC	492	2,00
Contra la intimidad	Ataques / interceptación sistemas y datos (art. 197 bis y ter)	47	0,19
	Difusión inconsentida de imágenes íntimas (art. 197.7)	78	0,32
	Descubrimiento/ revelación secretos a través TIC (art. 197)	399	1,62
Contra el honor	Calumnias/ injurias autoridades a través de TIC (arts. 215 y ss.)	129	0,52

Delitos informáticos		Procedimientos judiciales incoados	%
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (art 248 y 249)	20.111	81,68
	Descubrimiento secretos empresa a través de TIC (arts. 278 y ss.)	17	0,07
	Delitos c/ servicios de radiodifusión/interactivos (art 286)	42	0,17
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	134	0,54
	Delitos c/ propiedad intelectual a través de TIC (arts. 270 y ss)	84	0,34
De falsedad	Falsificación a través de las TICs	135	0,55
Contra Constitución	Discriminación a través de TIC (art. 510)	36	0,15
Otros		5	0,02
Total		24.622	100,00

Procedimientos por estafas y defraudaciones

Al igual que en años precedentes, el volumen más elevado de procedimientos judiciales por ciberdelitos corresponde a los incoados por hechos encuadrables en la categoría de estafas y defraudaciones, que alcanzaron la cifra de 20.111, un 81,68% del total de los registrados en el año entre los que abarca la competencia de la especialidad. Esta situación de preeminencia se viene constando año a año, y se va consolidando progresivamente, al elevarse en cada periodo anual dicho porcentaje. Es revelador que el indicador resultante de dicha comparación, que en el año 2019 fue del 65,52%, se haya elevado al 72,43% en el año 2020 y al 75,50% en 2021 hasta alcanzar la cifra de 81,68% en el año memorial. Por su parte, los datos que ofrece el Ministerio del Interior reflejan también cifras muy elevadas en referencia a las investigaciones policiales por actividades *online* de carácter defraudatorio que, en su comparación con el conjunto de delitos cometidos en el entorno virtual, ofrecen índices del 89,56% y 87,40% respectivamente en los años 2020 y 2021 y del 89,68% en el periodo anual objeto de esta Memoria.

No obstante, es obligado efectuar algunas precisiones a efectos de dimensionar adecuadamente la incidencia de estos ilícitos en el conjunto de la ciberdelincuencia. Así uno de los factores que sin duda

influye en esos abultados porcentajes es la habitualidad con la que estas conductas, a diferencia de otras manifestaciones criminales que no afloran con tanta facilidad, son objeto de denuncia por quienes se han visto afectados por ellas. De hecho, en los reiterados supuestos en los que, como consecuencia de la utilización de la red como medio de comisión, una misma conducta causa perjuicios a una pluralidad de personas ubicadas en el mismo o en distintos territorios, no es infrecuente que las denuncias presentadas por los distintos afectados den lugar a múltiples investigaciones policiales o judiciales que tienen por objeto aspectos parciales de una misma actividad criminal. Esta circunstancia puede determinar una diversidad de anotaciones estadísticas que, en inicio, se computan individualizadamente, aunque posteriormente, a resultas de la investigación, se acumulen en un solo procedimiento judicial. Es decir, en estos supuestos las anotaciones estadísticas parecen responder más a un registro de personas afectadas que de delitos efectivamente cometidos, sin que por nuestra parte sea posible depurar esa información y obtener resultados más precisos, al no contar con herramientas adecuadas para ello.

Por otro lado, hay que señalar que en la categoría correspondiente a las estafas y defraudaciones se integran una gran diversidad de actuaciones criminales que responden a dinámicas muy diferentes y que, por el momento, y dadas las carencias de nuestros registros informáticos tampoco estamos en condiciones de cuantificar separadamente. Así, junto a las estafas tradicionales cuya calificación como informáticas deriva del medio empleado para difundir el engaño como elemento vertebrador del tipo penal, se incluyen también en este apartado los denominados fraudes informáticos, es decir, acciones consistentes en manipular datos o sistemas informáticos para provocar un desplazamiento patrimonial no autorizado en perjuicio de otro, sin olvidar tampoco el variado elenco de manifestaciones criminales en las que los delincuentes combinan ambos factores –engaño y manipulación informática– con las grandes posibilidades de acción que ofrecen las tecnologías dando lugar a un repertorio inacabable de argucias de las que se sirven para lograr sus propósitos.

También se incluyen en esta misma categoría las conductas relacionadas con la utilización fraudulenta de medios de pago distintos del efectivo, materiales o inmateriales, cuya incidencia va incrementándose año a año favorecida por la articulación de nuevas tecnologías de pago y su uso habitual por los ciudadanos en el entorno virtual. Tanto es así que, a impulso de la normativa europea, el legislador español ha abordado por LO 14/2022 de 22 de diciembre la modificación de las figuras delictivas relacionadas con ello para hacer exten-

siva la tipificación penal al uso fraudulento de medios de pago de carácter inmaterial, así como a los actos preparatorios de estos ilícitos.

Obviamente, la consideración de todas estas circunstancias contribuye a relativizar, en alguna medida, los porcentajes obtenidos y permite una valoración más adecuada de la incidencia real de las estafas y defraudaciones en el conjunto de la actividad delictiva *online*, en el que se integran también otro tipo de manifestaciones criminales extremadamente peligrosas que luego se analizarán, sin perjuicio de reconocer el tremendo impacto social de los fraudes *online* por la elevada cuantía de los perjuicios que generan anualmente en el ámbito nacional e internacional.

De entre todas las formas de defraudación referidas anteriormente, siguen mereciendo un análisis detallado las que se estructuran a partir del engaño, cuya planificación y ejecución se ha visto potenciada por el uso generalizado de las comunicaciones electrónicas para la realización de todo tipo de actividades económicas o comerciales. Son muchos los ciudadanos que en los últimos años han resultado perjudicados económicamente, con ocasión de la contratación *online* de todo tipo de bienes o servicios ofertados falsamente. Las técnicas que emplean los/as delincuentes, aprovechando las posibilidades que ofrece la red para el anonimato o utilizando identidades supuestas, son cada vez más sofisticadas y difíciles de desentrañar para los investigadores, particularmente cuando la actividad ilícita, como es frecuente, tiene una dimensión internacional. La simulación de relaciones amorosas –*romance scam*, las cartas nigerianas, las propuestas estudiadamente sugerentes sobre vacaciones o actividades de esparcimiento, la apelación a los buenos sentimientos del internauta para provocar desembolsos con fines fingidamente sociales e incluso las ofertas de servicios de hackeo, son algunas de las maquinaciones que utilizan los defraudadores para captar la voluntad de sus futuras víctimas.

En este apartado se incluyen acciones ilícitas muy variadas y con marcadas diferencias en su planificación, dinámica criminal y en las dificultades para su esclarecimiento e identificación de sus autores. Entre las más sencillas o rudimentarias puede citarse la conocida policialmente como *operación zapatilla,* judicializada en 2022, relativa a la actuación de tres delincuentes que durante varios meses engañaron a otras personas ofertándoles *online* entradas para conciertos musicales o espectáculos públicos que previamente habían simulado y cuyo importe debía ser remitido a cuentas corrientes específicamente abiertas para ello. Pese a que el *iter criminis* carecía de especial complejidad y la cuantía del perjuicio individualmente causado tampoco era elevada, el

número de víctimas y su ubicación en distintos lugares de la geografía nacional hizo necesaria la intervención de la red de fiscales especialistas en labores de coordinación y determinación de los órganos judiciales territorialmente competentes para el conocimiento de los hechos.

En el extremo contrario, en atención a su dimensión transnacional y a las dificultades técnicas para su investigación, han de reseñarse las múltiples variantes de ofertas de inversión con las que los/las delincuentes intentan atraer a sus futuras víctimas simulando sólidas garantías de seguridad y una alta rentabilidad y para cuya contratación se exige normalmente la utilización de plataformas *online* y en muchas ocasiones que la operación se lleve a efecto en criptomonedas. La delicada situación económica existente en el marco nacional e internacional hace que estas propuestas resulten atractivas para un número creciente de ciudadanos/as que confiando en encontrar un cobijo seguro y rentable para sus ahorros realizan desembolsos económicos de diversa cuantía de los que los criminales se apropian, depositándolos en monederos fríos o desviándolos de su falso prometido destino hacia canales que les facilitan su ocultación. Las dificultades que ofrece la trazabilidad de los criptovalores en la *blockchain* y la identificación de quienes operan en ella añade una especial complejidad técnica a este tipo de investigaciones cada vez más numerosas. Ha de recordarse, no obstante que los recientes avances legislativos nacionales e internacionales en esta materia y la cooperación de organismos como Europol está contribuyendo a facilitar significativamente el curso y resultados de este tipo de investigaciones.

No podemos finalizar este análisis de las defraudaciones *online* articuladas en torno al engaño sin mencionar, al menos someramente, una circunstancia vinculada a este tipo de conductas y cuyos efectos perversos se incrementan año a año. Nos referimos a los supuestos en los que los/las delincuentes se sirven de datos personales ajenos, sustraídos u obtenidos con ocasión de contactos *online*, para utilizarlos en posteriores acciones criminales en la red, generando a los legítimos titulares de la identidad suplantada graves perjuicios y en muchas ocasiones múltiples reclamaciones judiciales como presuntos autores de actos ilícitos. Ofrecer soluciones efectivas ante estas situaciones requiere de mecanismos que permitan interrelacionar de forma automática la información derivada de los distintos expedientes, tarea en la que se encuentra actualmente inmerso el Ministerio del Interior. Entre tanto, desde la Unidad, estamos intentando paliar los efectos perversos que de ello se derivan para los afectados por estos comportamientos. A dicho fin se

incoan lo que llamamos *expedientes de suplantación de identidad* para recabar, a través de nuestras oficinas de enlace con los cuerpos policiales, información sobre estos supuestos y trasladarla a los/as fiscales delegados/as en los territorios en los que se siguen actuaciones contra los titulares de la identidad usurpada, a efectos de su oportuna valoración en los procesos en curso.

Aun cuando la necesaria brevedad de esta memoria nos impide explayarnos en demasía no podemos tampoco dejar de referirnos a la gran variedad de conductas defraudatorias en las que los/las delincuentes combinan hábilmente la manipulación informática con el engaño para conseguir sus ilícitos propósitos. Buen ejemplo de ello son los ataques *Business Email Compromise* (BEC), dirigidos generalmente contra entidades empresariales de cierta dimensión, cuya frecuencia está provocando importantes perjuicios económicos en España y en otros muchos países. En estos casos, los/las delincuentes tras obtener por medios diversos, entre ellos el acceso ilegal a sus sistemas, información sobre el funcionamiento interno de la entidad atacada, sus responsables y las operaciones comerciales en curso, suplantan la identidad de quienes gestionan el tráfico ordinario de la entidad, o de alguno de sus clientes o proveedores y ordenan en su nombre operaciones económicas *online*, aparentemente justificadas, desviando de esta forma importantes cantidades de dinero en su propio beneficio. También son significativos, por su frecuencia y por las peculiaridades de su *iter criminis*, los supuestos de la llamada *estafa del soporte técnico*, actividad en la que los/las agresores/as, mediante una intrusión irregular, infectan el dispositivo de la víctima y simulan un mal funcionamiento del sistema como justificación para dirigirse posteriormente a los/as afectados/as, fingiendo integrar el equipo técnico del proveedor del servicio, y ofrecerles la posibilidad de subsanar la disfunción detectada. Una vez captada la voluntad de la víctima, toman el control del sistema atacado, lo que les permite llevar a efecto sus criminales objetivos ya sea de exfiltrar información u obtener sus contraseñas o datos personales con finalidades diversas. Finalmente hemos de hacer mención a los supuestos en los que los/las delincuentes mediante la obtención irregular y posterior utilización de un duplicado de la tarjeta SIM de otra persona, logran vulnerar los mecanismos de seguridad de la banca *online* y, en consecuencia, autorizar directamente las operaciones fraudulentas que ellos mismos ordenan en perjuicio de la víctima y tener acceso, a través de los mensajes SMS, a los códigos de confirmación enviados por las entidades bancarias sobre las transacciones electrónicas realizadas.

Procedimientos por delitos contra la libertad sexual

Es esta una de las manifestaciones delictivas en la que se perciben con mayor claridad los efectos perversos del desarrollo tecnológico, particularmente en referencia a las agresiones a menores de edad, pues es evidente que las facilidades que ofrece la tecnología para mejorar la conectividad entre las personas y la transmisión de todo tipo de contenidos está favoreciendo indefectiblemente el acercamiento de los delincuentes sexuales a los/las menores con pretensiones de esa naturaleza y también la elaboración y difusión de material pornográfico infantil. Como consecuencia de ello todos los indicadores nacionales e internacionales sobre la materia vienen dejando constancia desde hace años del importante incremento de esta clase de actividades delictivas que se ha acentuado con un repunte, consecuencia de las medidas de confinamiento y aislamiento social adoptadas durante la pandemia causada por el COVID-19. Tanto es así que la Comisión Europea, el 27 de julio de 2020, dirigió una Comunicación al Parlamento Europeo, al Consejo y a otros altos organismos de la UE en la que llamaba la atención sobre esta circunstancia a la vista del *drástico aumento de denuncias por abusos sexuales de menores en línea en la Unión Europea,* al tiempo que proponía la elaboración en el marco comunitario de una Estrategia que haga posible *una respuesta firme y exhaustiva a estos delitos tanto en línea como sin conexión a Internet.* Dicha Estrategia se articula en torno a determinadas iniciativas que deberán ser desarrolladas durante el quinquenio 2020-2025 junto con otros planes de actuación actualmente en curso en el territorio comunitario.

Los delitos *online* contra la libertad sexual dieron lugar a la incoación de 1.507 expedientes judiciales que constituyen el 6,12% del total de procedimientos por ciberdelitos registrados en el año memorial. Esta cifra, muy levemente inferior a los 1.510 procedimientos registrados en 2021 pero algo superior a los 1.438 del 2020, se integra a su vez por 832 causas por delitos de pornografía infantil o de personas con discapacidad, 183 por *child grooming* y 492 por otra clase de ilícitos contra la libertad sexual, entre los que se incluyen las agresiones sexuales *online* a menores de edad o los actos de exhibicionismo.

Los procedimientos por actividades vinculadas a la pornografía infantil o de personas con discapacidad vienen ofreciendo en los últimos años unas cifras bastantes estables, aunque con una ligera tendencia al alza ya que el número de causas iniciadas en 2022 supera en 55, en cifras absolutas, las registradas en 2021 y en 125 las del año 2020. Este moderado ritmo de evolución parece contradecir las reflexiones

anteriormente expuestas acerca del importante crecimiento de estos ilícitos en el ámbito nacional e internacional. No obstante, esa aparente contradicción se explica fácilmente si tenemos en cuenta que las conductas de elaboración o distribución de material ilícito en el entorno tecnológico no son habitualmente objeto de denuncia por parte de los perjudicados/as, al tratarse de conductas clandestinas en las que las víctimas –habitualmente menores de muy corta edad– ni tan siquiera son conscientes de la agresión sufrida. De hecho, las investigaciones por estos ilícitos suelen iniciarse de oficio, a partir de comunicaciones de ciudadanos/as que detectan material de esta naturaleza en la red o de los reportes recibidos de determinados organismos como NCMEC o de cuerpos policiales de otros países, por lo que requieren de una intensa labor de indagación para corroborar la *noticia criminis* y obtener pruebas válidas y efectivas de la acción ilícita. Queremos decir con ello que no toda notificación recibida sobre hechos de esta naturaleza se logra materializar en investigaciones concretas, en ocasiones por falta de información suficiente y, en mayor medida, debido a la carencia de recursos personales y materiales adecuados para afrontar una actividad criminal en continua expansión que está siendo planificada y ejecutada a través de sistemas de comunicación cada vez más complejos y sofisticados –archivos compartidos en la nube, mensajería instantánea, redes Tor– y protegidos con sistemas de encriptación muy difíciles de quebrar. Una situación que demanda de una mayor concienciación social y un esfuerzo especial para dotar a Fuerzas y Cuerpos de Seguridad y también a los operadores jurídicos de mayor formación y medios legales y materiales más efectivos para mejorar la respuesta ante estos graves comportamientos.

Le siguen en importancia numérica en este apartado los procedimientos iniciados por cualquier otro delito *online* contra la libertad sexual, con 492 registros, categoría en la que se constata un crecimiento de casi el 19,4% respecto del año anterior. Dicho incremento puede tener su origen en las denuncias y/o investigaciones sobre actos de agresión sexual, generalmente a menores de edad, que se llevan a efecto a través de comunicaciones *online* y que, lamentablemente cada vez son más frecuentes. En sentido contrario las anotaciones estadísticas sobre expedientes relativos a delitos de *child grooming* descienden significativamente en casi un 43% desde las 321 del 2021 a las 183 registradas en el año memorial, circunstancia que aun siendo llamativa se explica en atención a la propia dinámica comisiva del hecho y a su tipificación penal. Al respecto ha de recordarse que lo que se sanciona en el actual art. 183 CP son actos preparatorios de agresiones sexuales a menores de 16 años, tanto en el entorno físico como virtual, o de ela-

boración, adquisición o distribución de material pornográfico infantil, conductas que, de llegar a producirse, serán objeto de anotación estadística preferente ya sea por su mayor gravedad o por que se produce una absorción del acto preparatorio por el finalmente resultante. Quiere decirse que, en un número no concretado de supuestos, el contacto con el menor a través de las TIC con fines de carácter sexual carece de reflejo estadístico cuando se logra la finalidad pretendida, al quedar integrado en la infracción más gravemente penada.

Procedimientos por delitos contra bienes personalísimos

Los actos *online* contra la libertad y seguridad de las personas dieron lugar en el año 2022 al inicio de un total de 1720 procedimientos, casi un 7% de los registrados por ciberdelitos. La cifra más elevada corresponde a los motivados por comportamientos encuadrables en los tipos penales más tradicionales de amenazas y coacciones si bien en este caso planificados y ejecutados en el entorno virtual, en tanto que 472 lo fueron por delitos de hostigamiento o acoso permanente, también conocidos como *stalking,* cometidos en todo o en parte a través de la red. Estas cifras dan cuenta de un significativo descenso, en poco más del 27%, respecto de las anotaciones efectuadas en esta categoría delictiva en 2021 que afecta esencialmente a las amenazas y coacciones ya que en los expedientes incoados por delitos del art. 172 ter el descenso se concreta únicamente en 18 procedimientos en cifras absolutas.

Esta disminución en el volumen de nuevas incoaciones de la que también da cuenta, aunque en un porcentaje inferior al 8%, la información facilitada por el Ministerio del Interior respecto de investigaciones policiales, implica una quiebra en la tendencia claramente alcista que se venía observando en los últimos años y que se concretó en el periodo interanual 2020-2021 en un repunte de más del 34%. No obstante, y en tanto dichos resultados no se confirmen en sucesivos periodos anuales, esta eventualidad ha de atribuirse a circunstancias puntuales ya que la progresiva generalización del uso de las tecnologías en toda clase de relaciones interpersonales permite augurar el inevitable traslado a la red de estas agresiones en todas sus variadas manifestaciones. A esos efectos no es baladí recordar que en muchas ocasiones y particularmente en los supuestos de *stalking*, este tipo de atentados contra la libertad y seguridad de las personas se enmarcan en situaciones de violencia de género materializándose en una pluralidad de acciones desarrolladas tanto en el entorno físico como virtual,

circunstancia que introduce un factor de aleatoriedad a efectos de su registro como competencia de esta área de especialidad, que bien podría justificar el descenso estadístico comentado.

Incluimos en este apartado, aunque se reconocen sus ocasionales matices próximos a las defraudaciones, las conductas de quienes aprovechando la conectividad que proporciona la red, simulan entablar una relación amorosa con otra persona determinándola a realizar frente a la videocámara acciones íntimas, básicamente de carácter sexual, que el delincuente graba sin consentimiento de la víctima y utiliza posteriormente para coaccionarla exigiéndole desembolsos económicos o la realización de actuaciones no deseadas. Ciertamente la argucia empleada para obtener las grabaciones y la circunstancia de que en ocasiones el/la responsable criminal ni tan siquiera tenga a su disposición esas imágenes, aunque así lo haga creer falsamente al afectado o afectada, permitiría argumentar una posible calificación como delito de estafa. Incluso, en algunos casos, cuando la pretensión del agresor/a es obligar a su víctima a realizar en su perjuicio un acto jurídico de disposición patrimonial pudiera plantearse su incardinación en la extorsión sancionada en el art. 243 CP. En estos supuestos, aun cuando la adecuada calificación jurídica de estas conductas dependerá de las concretas circunstancias concurrentes, en la especialidad nos decantamos generalmente hacia las tipologías que nos ocupan dado que el bien jurídico especialmente atacado es la libertad de acción de la víctima. En todo caso, se trata de conductas que preocupan especialmente por las ventajas que ofrece el entono virtual para su planificación y ejecución, por la intervención en su comisión de grupos de delincuencia organizada y por la asiduidad con la que se producen, causando serios perjuicios a los afectados/as no solo económicos sino especialmente de carácter moral, de tal gravedad que pueden llegar a poner en riesgo su propia vida como lamentablemente hemos constatado en alguna ocasión.

Por su parte el *stalking* sigue dando lugar a la incoación anual de un número importante y bastante estable de procedimientos penales. Las especiales e inacabables posibilidades de actuación que nos brindan las tecnologías favorecen la concurrencia de las exigencias de reiteración e insistencia que exige el art. 173 ter CP lo que determina que sea un tipo penal especialmente idóneo para su comisión en el ciberespacio. Posiblemente por ello el legislador, con ocasión de las últimas reformas del CP derivadas de la publicación de las Leyes Orgánicas 10/2022 y 1/2023, ha incorporado y posteriormente retocado, un quinto apartado en dicho artículo en el que se tipifica una conducta que, a diferencia de la prevista en los apartados primero a cuarto, solo es posible cometer a través de las TIC y que consiste en el uso de imágenes de otra persona

sin su consentimiento para realizar anuncios o abrir perfiles falsos de modo tal que se genere un situación de acoso o humillación para la víctima. Es evidente que con esta figura delictiva se pretende mejorar la acción penal frente a hechos de esas características, llamativamente frecuentes en la red, que hasta el momento no encajaban con facilidad en los tipos penales preexistentes.

Aun valorando positivamente esta iniciativa legislativa, a nuestro entender, constituye una respuesta meramente parcial ante la ausencia de una figura delictiva especifica que sancione en términos generales la suplantación *online* y en su perjuicio de la identidad de otra persona realmente existente, cuya tipificación se viene reclamando por la Fiscalía española desde hace varios años. Cierto es que algunos de los supuestos de usurpación de identidad ajena encuentran acogida en determinados tipos penales actualmente vigentes como es el caso del que acabamos de analizar o de las estafas a las que antes nos referíamos. Pero en otros muchos casos, en los que no concurren los requisitos exigidos por otras figuras delictivas, la usurpación *online* de la identidad de otro carece de respuesta en el ámbito penal y por tanto no puede ser objeto de persecución y sanción, aunque de ello se deriven consecuencias muy gravosas y lesivas para el honor o la intimidad de quien ha sido suplantado. Buena prueba de ello es que, según información publicada por el Gobierno Vasco, la Ertzaintza registró en 2022 un total de 843 denuncias por hechos de estas características, un 29 % más que en 2021, que en su mayoría hubieron de ser archivadas por falta de tipicidad. Estas cifras, aunque parciales, son reflejo de la incidencia real de estos comportamientos que se han visto favorecidos por las características inherentes a las comunicaciones virtuales y sobre cuyos perversos efectos han llamado la atención diversas directivas europeas.

También hemos de hacer mención en este apartado a los procedimientos por delitos contra la integridad moral, que sumaron 178 incoaciones en el año 2022, lo que supone un incremento del 74,5 % y del 125,3% respecto de los 102 y 79 expedientes incoados respectivamente en los años 2021 y 2020 e igualmente, en atención al bien jurídico protegido, a aquellos otros incoados por delitos contra la intimidad si bien muchas de sus manifestaciones aparecen estrechamente vinculadas a conductas tipificadas como ataques informáticos en los arts. 197 bis y ter CP. Estos ilícitos contra la intimidad dieron lugar a un total de 477 incoaciones, casi un 2% del total de procedimientos por ciberdelitos. De entre ellos, 78 tuvieron por objeto conductas incardinables en el art. 197.7 que sanciona la difusión no autorizada de imágenes o contenidos audiovisuales de carácter íntimo, previamente obtenidos con consentimiento de la víctima.

Procedimientos por delitos de ataques informáticos

Esta otra categoría de ilícitos se hace acreedora de un análisis específico por sus peculiares características y porque constituyen el núcleo duro de la ciberdelincuencia. Son figuras que aun cuando son objeto de tratamiento conjunto en la normativa europea, tanto del Consejo de Europa como de la propia Unión, han sido tipificadas por el legislador español en apartados distintos del código penal: como delitos contra la intimidad en los arts. 197 bis y ter o como delitos de daños informáticos, en los arts. 264 bis a ter.

El total de procedimientos registrados por estos ilícitos en 2022 asciende a 181 de los que 47 tuvieron por objeto conductas sancionadas como delitos contra la intimidad y los 134 restantes como daños informáticos. El análisis comparativo con los datos obtenidos en la anualidad precedente ofrece resultados dispares ya que, si bien se constata un significativo descenso, de poco más del 50%, en referencia a los procedimientos por hechos que pudiéramos denominar de espionaje informático, sancionados en los arts. 197 bis y ter CP, por el contrario, el cómputo de los expedientes relativos daños informáticos refleja un pequeño ascenso de poco más del 7% respecto del año precedente.

En cuanto a los primeros, hemos de hacer un razonamiento similar al efectuado anteriormente respecto del *child grooming*. Una buena parte de los accesos o interceptaciones ilícitas de comunicaciones electrónicas o de sistemas informáticos tienen como fin la intromisión no autorizada en la intimidad de otros, lo que da lugar a situaciones concursales que, a efectos de registro estadístico, determinan la anotación como delito contra la intimidad del art. 197 o incluso como delito de descubrimiento y revelación de secretos de empresa sancionado en el art. 278 CP si lo que se pretende con la intromisión irregular es la obtención de información reservada de entidades de esa naturaleza.

Ello no obsta para que demos la debida importancia a este tipo de comportamientos. Son acciones criminales cada vez más habituales y cuyos efectos pueden ser gravísimos no solo por su afección a la intimidad de las personas sino también por sus consecuencias económicas e incluso por el riesgo que pueden generar para la seguridad de instituciones públicas o del propio Estado. Buen ejemplo de ello es la actividad ilícita desarticulada en la reciente operación conocida como *Genesis market* que ha sido coordinada por Eurojust y Europol y en la que han participado autoridades policiales y judiciales de 17 países en su mayoría de la Unión Europea. Se trataba de una plataforma para la oferta y venta *online* de datos personales, irregularmente

obtenidos, de más de dos millones de ciudadanos/as, entre ellos múltiples credenciales para el acceso a sistemas *online* de muchas entidades públicas y privadas ubicadas en distintos lugares del mundo. Por nuestro país participaron conjuntamente miembros de las unidades especialistas en cibercrimen de Cuerpo Nacional de Policía y de la Guardia Civil contando con el apoyo y la coordinación de la Unidad, y se han intervenido como consecuencia de la operación datos e informaciones susceptibles de ser utilizados para la intromisión irregular en organismos públicos y entidades diversas ubicadas en España.

Por su parte y respecto a los actos de sabotaje informático, ha de destacarse la especial transcendencia y complejidad de algunos de ellos, particularmente los causados por ataques *ransomware* que han dado lugar a la incoación de varios procedimientos en distintos órganos judiciales. El mecanismo para canalizar el traslado de información sobre incidentes de seguridad que presenten caracteres de delito desde la Oficina de Coordinación de Ciberseguridad (OCC) del Ministerio del Interior a la Unidad de Criminalidad Informática, establecido por el art. 14.3 del Real Decreto Ley 12/2018 de 7 de septiembre, complementado por el Decreto-Ley 43/2021 de 26 de enero, está favoreciendo la posibilidad de actuación penal frente a estas conductas al tiempo que ha mejorado la capacidad de control y seguimiento de estas investigaciones.

Procedimientos por delitos de odio y contra la discriminación

Finalmente hemos de mencionar los 36 procedimientos incoados por delitos de odio y discriminación cometidos a través de las TIC de los que ha tomado conocimiento esta área de especialización y que han de sumarse a aquellos otros registrados en el ámbito competencial de la especialidad de los delitos de odio y contra la discriminación. La labor que corresponde en esta materia a los especialistas en Cibercrimen es la de apoyar a los integrantes de dicha área de especialización en la actuación frente a aquellos ilícitos que se cometen en el ciberespacio, así como desempeñar la función de punto nacional de contacto con los proveedores de servicio de internet que nos ha sido encomendada por el *Protocolo para la retirada de la red de contenidos relacionados con el discurso de odio* en el marco del Acuerdo Interinstitucional para colaborar en la Lucha contra el Racismo, la Xenofobia, la LGBTIfobia y otras formas de intolerancia, suscrito en septiembre de 2018.

Escritos de acusación

La información que ofrecemos en este apartado de la Memoria anual, al igual que la relativa a las diligencias de investigación penal tiene un interés muy especial a efectos no solo de analizar la evolución de la actividad criminal en el ciberespacio sino también para constatar la actuación del Ministerio Fiscal español frente a esta forma de criminalidad. Ha de reconocerse que la información derivada de estos registros carece de las notas de amplitud y generalidad que proporciona el análisis de los procedimientos incoados en el año pues la perspectiva que ofrece es mucho más limitada, pero su valor radica en que son datos tomados de actuaciones concretas realizadas por los/las fiscales en el ejercicio de sus funciones y, por tanto, escrupulosamente anotadas en nuestras aplicaciones informáticas, por lo que su fiabilidad es muy elevada.

Además, los escritos de acusación ofrecen la información que se toma como base para el cómputo estadístico, por lo que se encuentra mucho más depurada. Ya no se trata de denuncias, atestados o *noticias criminis* sobre sucesos presuntamente acaecidos y pendientes tanto de corroboración fáctica como de valoración acerca de su trascendencia penal, llegadas a conocimiento de los órganos judiciales o del Ministerio Fiscal, sino de escritos formulados por profesionales en los que se recoge la opinión de la Institución sobre la realidad de los hechos objeto de investigación, sus circunstancias y la calificación jurídica que les corresponde a partir de un estudio serio y reflexivo de los resultados obtenidos en la fase de instrucción judicial y de acuerdo con criterios de legalidad e imparcialidad.

Es decir, dichos escritos se refieren a supuestos en los que el/la especialista considera acreditada la realidad de los hechos que motivaron la iniciación del proceso, así como su carácter delictivo y su incardinación en un determinado tipo penal, por lo que su valor a los efectos que nos ocupan es incuestionable. Ciertamente, queda extramuros de este cómputo la información relativa a aquellas investigaciones en las que habiéndose corroborado plenamente la certeza de los hechos denunciados no ha sido posible, por unas u otras razones, dirigir la acción penal contra personas determinadas lo que da lugar a su sobreseimiento provisional.

En cualquier caso y a fin de una correcta valoración de los datos que ofrecemos es obligado precisar que, por deficiencias en el registro informático, aun cuando la acusación se formule por una pluralidad de ilícitos de igual o diferente naturaleza, generalmente solo se deja constancia estadística del más significativo de los mismos, des-

echándose la información sobre los restantes. En consecuencia, los datos registrados dan cuenta esencialmente del número de escritos de acusación presentados y de la figura delictiva principal o más grave que fue objeto de imputación en cada caso, pero no pueden considerarse reflejo exacto del volumen total de delitos que han sido objeto de acusación.

A partir de la información obtenida de los distintos órganos del Ministerio Fiscal, el número de escritos de acusación presentados en el año 2022 por delitos competencia del área de especialización asciende en conjunto a 4.089, 15 menos que en el año 2021, en el que se registraron 4.104 escritos de este tipo. Esta levísima disminución, en un 0,36%, carece de entidad para entender modificada la clarísima tendencia al alza que venimos detectando en número de acusaciones presentadas por ciberdelitos en los últimos años y que se refleja en un índice de crecimiento del 43,62% respecto de los 2.847 escritos de este tipo presentados en 2019 o del 27,50% respecto de los 3.207 de 2020.

El detalle de estos datos en atención a la calificación jurídica efectuada por el Ministerio Fiscal es el siguiente:

Delitos informáticos		Calificaciones	%
Contra la libertad	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss.)	336	8,22
	Acoso a través de TICs (art. 172 ter)	179	4,38
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)	345	8,44
	Acosos menores a través de TICs (art. 183 ter)	66	1,61
	Otros delitos c/libertad sexual a través de TIC	137	3.35
Contra la intimidad	Ataques/interceptación sistemas y datos (art. 197 bis y ter)	11	0,27
	Difusión inconsentida de imágenes íntimas (art. 197.7)	40	0,98
	Descubrimiento/ revelación secretos a través de TIC (art. 197)	234	5,72

Delitos informáticos		Calificaciones	%
Contra el honor	Calumnias/ injurias autoridades a través de TIC (arts. 215 y ss.)	13	0,32
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (arts. 248 y 249)	2520	61,63
	Descubrimiento secretos empresa a través de TIC (arts. 278 y ss.)	11	0,27
	Delitos c/ servicios de radiodifusión/interactivos (art. 286)	15	0,37
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	28	0,68
	Delitos c/ propiedad intelectual a través de TIC (art. 270 y ss.)	57	1,39
De falsedad	Falsificación a través de las TICs	57	1,39
Contra Constitución	Discriminación a través de TIC (art. 510)	17	0,42
Otros		2	0,05
Total		4.089	100,00

En coherencia con la información obtenida sobre las tipologías delictivas que generan mayor volumen de procedimientos, el número más elevado de escritos de acusación corresponde, un año más, a las estafas y defraudaciones, con 2.520 anotaciones, un 61,63% del total de los presentados en 2022. Llama la atención que aun cuando el volumen de acusaciones en el año memorial ha sido levemente inferior al de 2021, las relativas a delitos de estafa/defraudación se han incrementado en 238 en cifras absolutas respecto de la anualidad precedente. Sin perjuicio de ello, y como ya hemos indicado en anteriores Memorias, es preocupante el porcentaje resultante de la comparación entre el número de acusaciones efectivamente presentadas y el de procedimientos iniciados por estos ilícitos, que se sitúa en un 12,5%, dato que, si bien debe ser tomado con cautela ya que la acusación no suele formularse en el mismo año de incoación de la causa, es indicativo de la necesidad de mejorar la capacidad de respuesta frente a estas conductas.

Los delitos contra la libertad sexual en sus diversas manifestaciones dieron lugar a 548 escritos de acusación, un 13,40% del total de los presentados en 2022. De entre ellos, 66 corresponden a delitos de

child grooming y 345, el volumen más importante, a delitos de pornografía infantil o de personas con discapacidad cuyo número, no obstante, desciende ligeramente respecto de los 368 registrados en 2021. Por el contrario, las calificaciones elaboradas por otros delitos contra la libertad sexual fueron 27 más que en 2021 hasta alcanzar la cifra de 137. En cualquier caso, estimamos conveniente dejar constancia de la complejidad creciente de estas acusaciones motivada, entre otras razones, porque una parte muy importante de ellas tienen por objeto actos de agresión sexual y elaboración de material ilícito respecto de un número llamativamente elevado de víctimas.

En los delitos de esta naturaleza y con las salvedades antes indicadas el porcentaje resultante de la comparación entre escritos de acusación formulados y procedimientos incoados se eleva a casi un 37%, lo que da cuenta de una mayor eficiencia en el esclarecimiento de estas conductas e identificación de sus autores y desplaza la dificultad primordial para su persecución hacia problemas de *infradenuncia* y carencias en medios personales y materiales para abordar con éxito un mayor número de investigaciones.

Los delitos contra la libertad y seguridad de las personas –amenazas, coacciones y acoso permanente u hostigamiento– determinaron la presentación de 515 acusaciones, un 12,59% del total. También en este caso se detecta un claro descenso, en 79 escritos respecto del año 2021, que se manifiesta esencialmente en el apartado correspondiente a los delitos de amenazas y coacciones que dieron lugar a 83 escritos de acusación menos que en 2021. Por el contrario, las acusaciones referentes al delito del art. 172 ter ofrecen un levísimo incremento, concretado en 4 escritos, respecto del año anterior.

Las calificaciones por delitos contra la intimidad personal del art. 197, que suman en conjunto 274, aumentaron en poco más de un 14% respecto de las presentadas en 2021. El incremento se detecta tanto en las relativas a la difusión no autorizada de imágenes íntimas como en las que tuvieron por objeto cualquiera otras de las acciones tipificadas en dicho precepto, cuyo incremento es del 12,5%. Por su parte las relativas a los ilícitos de los arts. 197 bis y ter CP dieron lugar a 11 acusaciones, 2 más que en 2021. Al respecto ha de indicarse que en muchas ocasiones estas conductas aparecen en concurso con alguna otra de las sancionadas en el art. 197 dándose preferencia estadística a estas últimas por su mayor gravedad, lo que explica su reducido número.

Consideración aparte merecen las acusaciones presentadas en 2022 por delitos de daños informáticos que ascendieron a 28, con un incremento del 55% respecto de las formuladas en 2021. Aunque las cifras obtenidas en este apartado son todavía muy reducidas, en comparación

con el volumen de ataques que se producen anualmente, la obligación legal de muchos operadores de notificar los incidentes de seguridad que detecten y el mecanismo establecido para el traslado de esa información a los órganos de la jurisdicción penal cuando existan indicios de delito, está empezando a producir resultados positivos y favoreciendo la persecución penal de estos peligrosos comportamientos.

Diligencias de investigación penal

Aunque el número de estas diligencias es bastante reducido, su importancia es indiscutible al tratarse de actuaciones a través de las cuales el Ministerio Fiscal ejerce su capacidad investigadora para confirmar la realidad de determinados hechos que llegan a su conocimiento y realizar una primera valoración sobre su trascendencia jurídico penal a efectos de su ulterior traslado, si procediere, a la autoridad judicial competente para conocer de los mismos. Son actuaciones de naturaleza preprocesal, dirigidas directamente por los/las fiscales, que pueden incoarse de oficio o por denuncia de terceros y que tienen su soporte legal en los arts. 773.2.º de la LECrim y 5 de nuestro Estatuto Orgánico.

La tramitación de estas diligencias está limitada en su duración temporal por el art. 5 del Estatuto Orgánico y también por lo establecido en el citado art. 773-2.º que impone la remisión de las actuaciones al órgano judicial competente cuanto se constate la existencia de causa penal en curso por los mismos hechos. Además, la exigencia constitucional y legal de autorización judicial para realizar determinadas actuaciones que afectan a derechos fundamentales, impone la remisión de las diligencias a los órganos judiciales tan pronto como sea necesaria su práctica para la prosecución de la investigación.

El número de diligencias de esta naturaleza incoadas por ciberdelitos el pasado año ascendió a 218, cuyo detalle se especifica a continuación:

Delitos informáticos		Diligencias de investigación	%
Contra la libertad	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss.)	8	3,67
	Acoso a través de TICs (art. 172 ter)	10	4,59
Contra la integridad moral	Trato degradante a través de TICs (art. 173)	1	0,46

Delitos informáticos		Diligencias de investigación	%
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189)	11	5,05
	Acosos menores a través de TICs (art. 183 ter)	1	0,46
	Otros delitos c/libertad sexual a través TIC	13	5.96
Contra la intimidad	Ataques / interceptación sistemas y datos (art. 197 bis y ter)	1	0,46
	Difusión inconsentida de imágenes íntimas (art. 197.7)	3	1,38
	Descubrimiento/ revelación secretos a través de TIC (art. 197)	6	2,75
Contra el honor	Calumnias/ injurias autoridades a través de TIC (arts. 215 y ss.)	3	1,38
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (arts. 248 y 249)	118	54,13
	Descubrimiento secretos empresa a través de TIC (arts. 278 y ss.)	3	1,38
	Delitos c/ servicios de radiodifusión/interactivos (art. 286)	2	0,92
	Delitos de daños informáticos (arts. 264,264 bis y 264 ter)	5	2,29
	Delitos c/ propiedad intelectual a través de TIC (arts. 270 y ss)	1	0,46
De falsedad	Falsificación a través de las TICs	10	4,59
Contra Constitución	Discriminación a través de TIC (art. 510)	22	10,09
Otros		0	0,00
Total		218	100,00

También en este caso, la cifra más elevada de incoaciones corresponde a las incoadas por estafa y defraudación que suponen un 54,13% del total de las registradas. Destacan igualmente las 25 incoadas por delitos contra la libertad sexual, un 11,4% del total, así como las 22 que tuvieron su origen en delitos de odio y/o discriminación a través de la red que suponen poco más del 10% de las registradas en el año.

Con un porcentaje inferior, que no llega al 9% ha de hacerse mención a las diligencias incoadas por delitos contra la libertad y seguridad de las personas, 8 por amenazas y 10 por delitos de acoso permanente u hostigamiento.

En la Unidad Coordinadora se incoaron un total de 5 diligencias de investigación, 4 de ellas a efectos de determinar el órgano territorialmente competente para el conocimiento de los hechos, al amparo de lo establecido de la entonces vigente Circular 4/2013 FGE, por lo que logrado ese objetivo todas ellas fueron trasladadas al órgano del Ministerio Fiscal correspondiente en atención a los resultados obtenidos. La última de las indicadas, relativa a un supuesto delito de daños informáticos, en la que la investigación fue encomendada a esta Unidad por Decreto de 8 de marzo de 2022 de la Excma. Sra. Fiscal General del Estado, resulto finalmente archivada al no existir indicios de la comisión de los hechos denunciados.