8.2 Análisis de las diligencias de investigación y procedimientos judiciales incoados y acusaciones formuladas por el Ministerio Fiscal en el año 2025

Nuestras reflexiones acerca de la actuación jurisdiccional y del Ministerio Fiscal en esta materia durante el año 2025 se basan en la experiencia adquirida y en los datos obtenidos por los integrantes de la red de fiscales especialistas en criminalidad informática –casi 190 en todo el territorio del Estado– con ocasión del ejercicio de sus funciones, tanto en actuaciones propias de la institución como en las intervenciones que nos competen en los procesos judiciales. Combinamos por tanto en este análisis información procedente de la propia Fiscalía con aquella otra derivada de la incoación y tramitación de procedimientos penales, con la pretensión de ofrecer, desde el punto de vista de la jurisdicción penal, la mayor aproximación posible a la dimensión real de la ciberdelincuencia en el último periodo anual y a la incidencia que sus múltiples manifestaciones están teniendo en los derechos e intereses de la ciudadanía y en el desenvolvimiento de la actividad social.

Repasaremos no solo la evolución de los que se consideran ciberdelitos *stricto sensu*, al tratarse de acciones que inciden directamente en elementos informáticos, sino también de aquellos otros en los que los agresores se sirven de las tecnologías para atentar contra bienes jurídicos personalísimos como la intimidad, la libertad y seguridad, la integridad moral, el honor o la libertad sexual. Sin olvidar tampoco los numerosos ilícitos *online* que afectan a intereses económicos o patrimoniales, como estafas y defraudaciones, o los que ponen en riesgo intereses colectivos o difusos, como el uso del entorno digital con finalidades terroristas o para la difusión del discurso de odio.

Ciertamente las competencias del área de especialización contra la criminalidad informática están claramente definidas en la Instrucción de la FGE núm. 2/2011, de 11 de octubre, *sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías,* actualizada en 2021, pero ha de reconocerse que en no pocas ocasiones la determinación de si una concreta conducta puede o no ser catalogada como ciberdelincuencia no es cuestión sencilla, particularmente al inicio de la investigación criminal cuando todavía no se han perfilado suficientemente los contornos de la acción ilícita.

Todas las circunstancias antedichas dificultan la labor de reflexión y análisis que nos ocupa, que tropieza además con los

serios inconvenientes derivados de las innumerables carencias y disfunciones de nuestros sistemas y aplicaciones informáticas. Hemos de lamentar que estas deficiencias impliquen un incuestionable lastre a efectos de aprovechar plenamente el enorme volumen de información del que dispone la Fiscalía que, en condiciones óptimas, nos permitiría realizar un estudio completo y detallado de la situación de la ciberdelincuencia en nuestro país y de su evolución año a año. Como indicábamos en la Memoria de 2024, la configuración de la Fiscalía española, como una institución centralizada con intervención obligada en la mayoría de los procesos penales y provista por disposición estatutaria de una especial capacidad de coordinación interna y de trabajo en equipo, nos coloca en una posición única, en un observatorio privilegiado, para la valoración de este fenómeno criminal. Sin embargo, la insuficiencia de nuestras aplicaciones informáticas y las clamorosas diferencias en los sistemas previstos en las distintas CCAA para el control y seguimiento de las causas, hace que la recopilación de datos estadísticos resulte especialmente difícil y que se produzcan «fugas» de información, particularmente en algunos territorios.

Con todo, ha de reconocerse que el trabajo serio y esforzado de quienes integran la red de fiscales especialistas, concretado en muchos territorios en un control y seguimiento personal y casi artesanal de los expedientes, ha permitido subsanar algunas carencias y completar –al menos parcialmente– los datos estadísticos, frecuentemente incompletos, obtenidos de las aplicaciones informáticas. En consecuencia, no podemos afirmar que los datos que ofrecemos sean exactos, pues somos conscientes de las limitaciones antes indicadas, pero sí podemos asegurar que, aun incompletos, constituyen una información contrastada y adverada por los propios fiscales en sus respectivos territorios y que por ello ofrecen una aproximación de especial interés para valorar la evolución de la ciberdelincuencia que, al igual que en años anteriores, analizaremos separadamente en atención a las distintas categorías delictivas.

Pues bien, según la información recopilada sobre procedimientos judiciales y diligencias de investigación del Ministerio Fiscal registrados por cualquiera de las conductas delictivas competencia del área de especialización, tal y como queda definida en la Instrucción 2/2011 antes citada, en 2025 se iniciaron en el conjunto del territorio del Estado 33.851 procedimientos judiciales y 499 diligencias de investigación del Ministerio Fiscal, lo que hace un total de 34.350 expedientes por ilícitos encuadrables en el concepto de ciberdelincuencia. Esta cifra supone en conjunto un incremento del 24,69% en

referencia a los datos obtenidos en 2024, anualidad en la que se registraron 27.547 expedientes de este tipo (27.104 causas judiciales y 443 diligencias de investigación), siendo significativo el repunte en el número de causas judiciales, ya que en el año memorial se incoaron 6.747 procedimientos más que en 2024, lo que revela un indicador al alza de casi el 25%.

Seguimos por tanto detectando la imparable tendencia alcista de la que vamos dando cuenta año a año, si bien en esta ocasión en porcentajes más elevados que en otras ocasiones. De hecho, a excepción de la leve inflexión (de un 4,61%) en el número de expedientes incoados en 2023, en los últimos ejercicios venimos constatando un crecimiento más o menos marcado que se concretó, por ejemplo, en un 14,86% en el año 2024 o en un 3% en 2022. No obstante, fue con ocasión del análisis correspondiente al año 2021 (primer periodo anual posterior a la pandemia de la COVID-19) cuando el indicador de crecimiento fue especialmente elevado al alcanzar el 40,47% respecto a la cifra de incoaciones del año 2020, posiblemente como consecuencia de la ralentización en la tramitación de procedimientos judiciales en ese periodo anual y de la mayor digitalización de las relaciones interpersonales generadas. En cualquier caso, es significativo que en el último quinquenio –años 2021 a 2025– el número de procedimientos y/o diligencias de investigación del Ministerio Fiscal se haya incrementado en un 42,4% al evolucionar desde los 24.126 que se registraron en 2021 a los 34.350 incoados en 2025.

Estos datos se ven corroborados por la información que reflejan los balances anuales sobre cibercriminalidad del Ministerio del Interior, según los cuales, y con las salvedades derivadas de la inclusión en el cómputo de investigaciones no judicializadas, el incremento de actuaciones policiales por ciberdelitos en ese mismo quinquenio es de más del 60%, lo que explica también que la incidencia de la ciberdelincuencia en el conjunto total de la delincuencia haya ascendido del 16,3% del año 2021 al 19,85% registrado en el cuarto trimestre del 2025.

El detalle de los resultados relativos a la incoación de causas judiciales en atención a las distintas tipologías delictivas queda reflejado en el cuadro:

Delitos informáticos		Procedimientos judiciales incoados	%
Contra la libertad.	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss.).	1.614	4,77
	Acoso a través de TICs (art. 172 ter).	464	1,37
Contra la integridad moral.	Trato degradante a través de TICs (art. 173).	73	0,22
Contra la libertad sexual.	Pornografía infantil/discapaces a través de TICs (art. 189).	865	2,56
	Acoso menores a través de TICs (art. 183).	160	0,47
	Otros delitos c/libertad sexual a través TIC.	570	1,68
Contra la intimidad.	Ataques/interceptación sistemas y datos (art. 197 bis y ter).	100	0,30
	Difusión inconsentida de imágenes íntimas (art. 197.7).	204	0,60
	Descubrimiento/revelación secretos a través TIC (art. 197).	356	1,05
Contra el honor.	Calumnias/injurias autoridades a través TIC (art. 215).	32	0,09
Contra el patrimonio y el orden socio-económico.	Estafa cometida a través de las TICs (arts. 248 y 249).	28.952	85,53
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss.).	35	0,10
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286).	14	0,04
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter).	146	0,43
	Delitos c/ propiedad intelectual a través TIC (arts. 270 y ss.).	38	0,11
De falsedad.	Falsificación a través de las TICs.	164	0,48
Contra Constitución.	Discriminación a través TIC (art. 510).	18	0,05
Otros.		46	0,14
Total.		33.851	100,00

8.2.1 Procedimientos judiciales por delitos de estafa y defraudación

Al igual que en ejercicios anteriores, las estafas y defraudaciones son las tipologías delictivas que dieron lugar a un número más elevado de incoaciones durante el año. En 2025 se registraron un total de 28.952 causas penales por hechos ilícitos encuadrables en los artículos 248 y ss. del CP, es decir, un 85,53% del total de procedimientos judiciales por ciberdelitos.

Este último indicador, pese a ser llamativamente elevado, no implica más que un ligero ascenso respecto de los índices obtenidos en años anteriores: 83,43% en 2024, 82,87% en 2023 o 81,68% en 2022. Es decir, esta especial prevalencia de las investigaciones por delitos de carácter defraudatorio la venimos observando desde el inicio de nuestra actividad especializada contra la ciberdelincuencia. En la memoria del año 2011 ya dejamos constancia de que las causas por estos ilícitos suponían el 64,36% de la actividad jurisdiccional contra la ciberdelincuencia y desde entonces los indicadores porcentuales han ido subiendo de forma más o menos pronunciada, pero con un ritmo progresivo y constante. Concretamente, entre los años 2021 y 2025 el volumen de estos expedientes en la jurisdicción penal ha crecido en conjunto en un 61,12%, cifra muy similar a la que resulta de los informes del Ministerio del Interior sobre investigaciones policiales que se concreta en el 61,22%.

La cifra de 28.952 procedimientos por actividades defraudatorias en cualquiera de sus manifestaciones supone la incoación en el año memorial de 6.338 expedientes más que en 2024 y 9.488 más que en 2023. Este incremento en las dos últimas anualidades pudiera tener su origen, al menos en parte, en la modificación de nuestro Código Penal por la LO 14/2022, de 22 de diciembre, resultante de la implementación de la Directiva (UE) 2019/713, de 17 de abril, *sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo*, uno de cuyos efectos fue la supresión en estos ilícitos de la cláusula que otorga el carácter de leve a aquellas infracciones cuya cuantía sea inferior a 400 euros, salvo en los casos en que el desplazamiento patrimonial se base exclusivamente en el engaño.

Pese a la rotundidad de estos datos estadísticos, su interpretación exige algunas matizaciones para evitar la errónea conclusión de que en la generalidad de los supuestos –salvo escasas excepciones– la finalidad que se pretende con la delincuencia en la red es de carácter defraudatorio. Desde nuestro punto de vista estos llamativos resultados se deben, en buena parte, a que las estafas y defraudaciones son

los ilícitos que más se denuncian dada la facilidad con que los propios perjudicados pueden percibir el carácter fraudulento de la actividad. No ocurre lo mismo con otros ilícitos también habituales en la red, como los que atentan contra la libertad sexual de menores, los relacionados con el discurso de odio o los ataques informáticos, que por razones diversas –ya sea la especial vulnerabilidad de las víctimas o el temor del afectado a la pérdida de reputación o prestigio– no son objeto de denuncia y, por tanto, no llegan a conocimiento ni de los investigadores ni de los órganos de la jurisdicción penal.

También influye en estos resultados la circunstancia, notablemente frecuente, de que los múltiples perjudicados de una misma acción ilícita presenten individualmente denuncia, incluso en distintos territorios, dando lugar a registros estadísticos independientes, computables como tales, aunque posteriormente la investigación del ilícito se realice en una causa única común para todos los afectados. Finalmente, también ha de recordarse que la sección del Código Penal dedicada a las estafas incluye una gran variedad de conductas delictivas con planteamientos y dinámicas comisivas muy diversas, como ahora veremos, aunque coincidan en un elemento común que es el que determina su inclusión en la misma categoría delictiva: el desplazamiento económico no autorizado en perjuicio de la víctima y en beneficio del delincuente o de un tercero. Es por ello por lo que las investigaciones penales que se encuadran en este grupo son incuestionablemente numerosas.

Con estas reflexiones no pretendemos minimizar un fenómeno criminal que preocupa extraordinariamente a nivel nacional e internacional por los graves perjuicios económicos que ocasiona anualmente y por el riesgo de una eventual pérdida de confianza de los ciudadanos en el comercio electrónico y la economía digital. Nuestra única pretensión es facilitar la correcta interpretación de las cifras que ofrecemos y la adecuada valoración del alcance efectivo las diversas actividades delictivas que se planifican y ejecutan en el entorno virtual.

Otra de las consecuencias de la última reforma del Código Penal es la nueva estructuración de las figuras delictivas, de modo que el art. 248 CP castiga las estafas tradicionales, basadas en el engaño a la víctima, en tanto que el art. 249 CP tipifica aquellas otras en que el desplazamiento patrimonial trae causa de una manipulación informática y/o del uso irregular de medios de pago distintos del efectivo.

Ello no debe llevarnos a concluir que las estafas tradicionales quedan en todo caso fuera del ámbito de competencia de la red especializada en cibercrimen, ya que es incuestionable que la capacidad de

acción que ofrecen las tecnologías está contribuyendo decisivamente no solo a la rápida difusión del engaño, sino también a ejecutarlo de forma más sofisticada y convincente y, por tanto, con mayores posibilidades de captar la voluntad de terceros e inducirles a realizar un desembolso económico perjudicial. Así ocurre, entre otros supuestos, cuando se utiliza la farsa de imaginarias inversiones en criptomonedas como «gancho» para atraer a las víctimas, en los fraudes cometidos mediante «*bizum* inverso» o en las múltiples variantes de utilización de la IA con dicha finalidad.

En cualquier caso, es evidente que el recurso a las tecnologías está favoreciendo la actividad criminal de los defraudadores. Persiste la utilización de plataformas de comercio electrónico o de intermediación entre particulares para ofertar fraudulentamente bienes y servicios, ya se trate de publicitar productos inexistentes o de simular características o propiedades de las que carecen, con el objetivo de beneficiarse con los desembolsos que realizan quienes engañados contratan su adquisición. La facilidad con que se planifican y ejecutan estas actividades, su rápida difusión en la red y la posibilidad de afectación a una pluralidad de víctimas en distintos territorios, hace que estos comportamientos sigan siendo frecuentes en el entorno virtual y que su investigación ofrezca dificultades derivadas, precisamente, de la atomización y dispersión de los perjuicios causados, lo que obliga a un especial esfuerzo de coordinación que en múltiples ocasiones asumimos como área de especialización.

Junto a estas supercherías más tradicionales, las aplicaciones de IA han venido a mejorar la capacidad de engañar a terceros, ya que permiten imitar estilos de escritura, eliminar errores y, en definitiva, crear contenidos altamente convincentes. Así está ocurriendo, por ejemplo, con los ataques de *phishing* avanzado, en los que a partir del estudio de gran cantidad de datos es posible personalizar la agresión y, por ende, hacer más creíble el engaño para el receptor de la comunicación. Y lo mismo ocurre en los casos vulgarmente conocidos como «estafas del hijo en apuros», en que mediante estas herramientas de IA se simula con gran realismo la intervención de personas íntimamente relacionadas con la víctima –familiares o amigos– para inducirle a realizar un desembolso económico ante una simulada situación de urgencia, o en aquellos otros en los que el suplantado es un personaje conocido y famoso en el ámbito de la política o de las finanzas que recomienda a futuros inversores operaciones financieras supuestamente ventajosas y en apariencia de alta rentabilidad.

Pero posiblemente el volumen mayor de conductas encuadrables en esta categoría delictiva se corresponde con la utilización fraudu-

lenta de medios de pago distintos del efectivo, ocasionalmente tras ser falsificados o alterados, y también por el uso no autorizado de sus datos, irregularmente obtenidos, para la realización *online* de operaciones económicas de carácter ilícito. Son conductas sancionadas en el art. 249.1.b) CP, según la redacción dada a este articulo por la última reforma del Código Penal, que, en el apartado 2.b) del mismo precepto, extiende incluso la criminalización a los actos preparatorios de dichos comportamientos y cuya investigación resulta especialmente compleja, al igual que la determinación de sus responsables, dado que muchas veces el uso fraudulento se materializa en operaciones transnacionales. Por ello, en innumerables ocasiones, las denuncias por estos ilícitos ni tan siquiera son trasladadas a los órganos de la jurisdicción penal ante la ausencia de vías de investigación que hagan posible la identificación de sus autores.

Por su parte, la definición legal de la estafa informática en la normativa internacional –art. 8 del Convenio de Budapest y art. 6 de la citada Directiva (UE) 2019/713– y su tipificación en las legislaciones internas, entre ellas en nuestro art. 249.1.a) CP, ha hecho posible la respuesta penal en aquellos supuestos en que el desplazamiento patrimonial no se produce mediante engaño sino a consecuencia de acciones no autorizadas sobre datos y sistemas informáticos. Es el caso del *pharming*, en el que el agresor redirige el tráfico a un sitio web falso con el objetivo, por ejemplo, de apoderarse de contraseñas o claves bancarias para su posterior uso fraudulento. En estos casos, a diferencia del *phishing*, no es necesario que la víctima actúe de una forma determinada, pues el efecto pretendido se logra directamente mediante manipulación del DNS (*Domain Name System* o sistema de nombres de dominio) o aprovechando las vulnerabilidades del propio sistema informático atacado.

No obstante, los supuestos más habituales son aquellos en los que los agresores combinan la manipulación informática con diversas formas de engaño a la víctima para lograr el desplazamiento patrimonial pretendido. Uno de los ejemplos más característicos, junto alguno de los mencionados, es el fraude del CEO o BEC (*business email compromise*), que es una amenaza creciente en nuestro país y a nivel mundial por los graves perjuicios que está generando.

En estos casos los atacantes estudian el funcionamiento y estructura de la entidad objeto de la agresión, ya sea accediendo irregularmente a sus sistemas o también aprovechando información de fuentes abiertas o de la propia web corporativa, hasta conocer la forma en que se ordenan, canalizan y ejecutan sus operaciones económicas, así como el estado de sus cuentas. Adquirido un conocimiento suficiente

sobre ello, los atacantes ordenan actuaciones en perjuicio de la empresa y en favor de cuentas propias usurpando a dicho fin –mediante correos electrónicos simulados o incluso *deepfakes*– la identidad de quien está habilitado para emitir ese tipo de órdenes. En otros casos, los suplantados son directivos o gestores de empresas titulares de créditos pendientes con la entidad atacada, supuestos en que los agresores arteramente sustituyen las cuentas fijadas para el pago por otras a su disposición, en las que finalmente se ingresan las cantidades adeudadas. A la dificultad que entraña el esclarecimiento de estas ilícitas actividades, se añade el desafío de evitar el efectivo desplazamiento económico y que los fondos fraudulentamente obtenidos sean enviados a ciertos países donde, por deficiencias en la cooperación, no sea posible su recuperación. Solventar estas situaciones es uno de los objetivos en los que nos encontramos empeñados en colaboración con las fuerzas y cuerpos de seguridad y las entidades bancarias.

Las defraudaciones en operaciones de la banca *online* cada vez son más frecuentes y también generan importantes perjuicios económicos ya que el desarrollo del comercio electrónico y de la economía digital ha traído consigo un incremento de estos ilícitos que ofrecen múltiples variantes. La apertura de cuentas bancarias usurpando identidades ajenas y su utilización posterior como soporte para solicitar créditos o realizar operaciones con cargo a las mismas es, con frecuencia, objeto de investigación penal. Tanto es así que estas simulaciones de identidad han llamado la atención de la oficina del Defensor del Pueblo hasta el punto de determinar la celebración de una reunión de trabajo con integrantes de la Fiscalía General y de esta Unidad para buscar soluciones legales u operativas que mejoren la respuesta ante estas situaciones.

También en este ámbito se están dejando notar los efectos del uso irregular de la IA. Acciones tales como crear documentos, fotografías o vídeos falsificados, para eludir los controles de identificación y verificación de los clientes de instituciones financieras, o combinar dichos contenidos generados por IA con información personal legítima, irregularmente obtenida, para crear identidades sintéticas, son un buen ejemplo de ello y resultan de extraordinaria utilidad para abrir cuentas con identidades falsas u ordenar trasferencias económicas sustituyendo al titular legítimo y, en general, para ejecutar acciones fraudulentas no solo en el ámbito bancario sino en cualquier actividad del comercio electrónico.

Asimismo son frecuentes los ataques de *phishing* en los que se simula una comunicación proveniente de fuentes confiables, en ocasiones de las propias entidades bancarias, para obtener de los usuarios

de servicios de pago las contraseñas y/o credenciales que permitan a los delincuentes ordenar ilícitamente operaciones económicas. Este tipo de ataques, inicialmente de carácter masivo, han evolucionado haciéndose cada vez más personalizados (*spear phishing*), proceso favorecido por la utilización de aplicaciones de IA que permiten recabar previamente cantidades ingentes de información sobre el comportamiento *online* de la futura víctima.

El incremento de los fraudes en las operaciones de banca *online* ha determinado la elaboración en el seno de la UE de una nueva Directiva (PSD3) y un Reglamento (PSR) sobre servicios de pago, aún pendientes de aprobación, con la finalidad de reforzar las técnicas y medidas de seguridad destinadas a reducir o evitar el fraude en estas operaciones. También en nuestro país, en los últimos años se han ido generando interesantes debates acerca de la suficiencia de las medidas legalmente previstas a estos efectos e incluso se han publicado algunas resoluciones judiciales –entre ellas la STS, Sala Primera, 571/2025, de 9 de abril– en las que se fijan criterios acerca de la posible responsabilidad en que pudieran incurrir los prestadores de servicios de pago en supuestos de insuficiencia de las medidas de seguridad adoptadas. Asimismo, por nuestra parte se analizó esta materia junto con técnicos del Banco de España en una de las sesiones de trabajo de las Jornadas de Fiscales Especialistas en Criminalidad Informática del pasado año 2025, dando lugar a la propuesta de algunos criterios de actuación recogidos en una de las conclusiones adoptadas en las mismas.

Tampoco podemos dejar de mencionar en este breve repaso las acciones de quienes se sirven de los servicios de telecomunicación, como es el caso del *vishing*, mediante llamadas de voz, o del *smishing*, a través mensajes de texto SMS o WhatsApp, para embaucar a la víctima e inducirla a contratar productos o servicios inexistentes o fraudulentos o para obtener de ella información personal o de carácter financiero que pueda utilizar el atacante en propio interés. En uno y otro caso quien entabla la comunicación suele simular que actúa en nombre de empresas, organismos o instituciones de confianza y para ello se sirve de la manipulación del identificador de la línea llamante o de los mensajes cortos SMS o MMS. La frecuencia de estas conductas, con los correspondientes perjuicios para las víctimas y los efectos negativos que pueden producir en la deseable confianza de la ciudadanía en la seguridad de las comunicaciones y en la actividad comercial *online,* dieron lugar en el año memorial a la publicación de la Orden Ministerial TDF/149/2025, de 12 de febrero, que impone a los operadores de comunicaciones la obligación de bloquear aquellas llamadas o mensajes cortos que presenten signos de manipulación o de origen

dudoso. También en referencia al uso irregular de los servicios de telecomunicación es obligada la mención de la técnica *SIM swapping*, en la que el atacante consigue irregularmente un duplicado de la tarjeta SIM de otra persona, posibilitando de esta forma la interceptación de sus llamadas, mensajes y códigos de seguridad y, por ende, el acceso a sus cuentas bancarias. Esta forma de defraudación ha determinado la incoación un número significativo de investigaciones y procesos penales en los últimos años, si bien el reforzamiento de las medidas de seguridad por parte de las entidades bancarias y los operadores de comunicaciones ha contribuido a dificultar y a reducir estas ilícitas actividades.

8.2.2 Delitos de ataques a datos y sistemas informáticos

Los ataques a datos y sistemas informáticos están tipificados en nuestro Código Penal en los arts. 264 y 264 bis, si la acción consiste en un acto de sabotaje informático; en el art. 197 bis, cuando lo que se pretende es el acceso irregular a un sistema informático o la interceptación de comunicaciones entre sistemas; y en los arts. 197 ter y 264 ter cuando se trata de actos preparatorios de unos y otros.

Los que definimos como sabotajes informáticos dieron lugar a la incoación en 2025 de un total de 146 procedimientos judiciales, un 0,43% del total de los incoados por ciberdelitos. Esta cifra da cuenta de un ligero aumento en tan solo 9 procedimientos respecto de los 137 incoados en 2024; de 16 en referencia a los 130 de 2023 y de 21 respecto de los registrados en 2021. Por tanto, es evidente que, aun cuando la incidencia de estos procedimientos aumenta progresivamente, su número sigue siendo reducido en las estadísticas judiciales.

Tradicionalmente estas agresiones no llegaban con facilidad a conocimiento de los órganos de la jurisdicción penal ya que los afectados, en no pocas ocasiones, optaban por no denunciarlos por motivos de carácter reputacional. Sin embargo, la publicación de la Directiva (UE) 2016/1148, de 6 de julio, *relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión* –conocida como NIS 1– y su implementación en España por el Real Decreto-ley 12/2018, de 7 de septiembre, supuso un punto de inflexión al establecer para determinados operadores la obligación de notificar a los organismos competentes los incidentes de seguridad que afectaran a sus redes y sistemas, obligación esta cuya ampliación a otras entidades y empresas está siendo objeto de estudio con ocasión de la tramitación del Antepro-

yecto de Ley de Coordinación y Gobernanza de la Ciberseguridad con el que se pretende implementar internamente la Directiva (UE) 2022/2555 –NIS 2–. Pues bien, esta notificación de incidentes, junto con la previsión que establece el art 14.3 del citado Real Decreto-ley 12/2018 según la cual la Oficina de Coordinación en Ciberseguridad (OCC) ha de comunicar a los cuerpos policiales y a esta Unidad contra la Criminalidad Informática los incidentes de seguridad de carácter delictivo llegados a su conocimiento por mor del citado deber de notificación de los sujetos obligados, está favoreciendo la investigación de estos ataques y, por ende, la posibilidad de actuar penalmente frente a sus responsables.

En cualquier caso, ha de recordarse que la respuesta penal a este tipo de fenómenos es muy compleja y todavía en demasiadas ocasiones las diligencias policiales para su esclarecimiento no ofrecen resultado positivo, por lo que en un número no determinado de supuestos dichas investigaciones no llegan a judicializarse al no existir vías para la identificación del autor, lo que explicaría que el número de causas judiciales por estos ilícitos sea todavía muy reducido.

Los ataques más frecuentes, y que generan perjuicios más graves a nivel nacional e internacional, son los que se sirven del tipo de *malware* denominado *ransomware,* cuyo principal efecto es el cifrado de los datos o sistemas haciéndolos inaccesibles, de forma que su titular no pueda disponer ni acceder a la información almacenada salvo que acceda a abonar el rescate que exigen los agresores, ocasionalmente en criptomonedas. En los últimos años la utilización de este *malware* ha ido evolucionado y dando lugar a efectos cada vez más peligrosos: el de doble extorsión, cuando al tiempo del ataque los delincuentes se apoderan de información sensible que amenazan con publicar si no reciben una ventaja económica o, incluso, el de triple extorsión, si además los agresores amenazan con lanzar ataques *DDoS* para presionar más gravemente a sus víctimas.

Como también ha ido evolucionando el modo de selección de las víctimas, de tal modo que el *ransomware* común, que concreta sus objetivos de forma indiscriminada, se ha ido sustituyendo por el *ransomware* dirigido, que está siendo utilizado preferentemente contra las pymes, aprovechando que generalmente disponen de recursos limitados en ciberseguridad y de menor capacidad de recuperación ante estos incidentes por lo que son más vulnerables que las grandes corporaciones. El último paso en esta evolución está vinculado al uso de la IA y el incremento del *ransomware as a service –RaaS–* es decir, la venta de herramientas que facilitan a terceros la realización de estos ataques aun careciendo de conocimientos técnicos para ello, uno de

cuyos productos es el *LockBit3*, *ransomware* diseñado específicamente para dificultar su detección. Otra forma de sabotaje informático son los ataques *DDoS* (*Distributed Denial of Service*), cuyo objetivo es anular la operatividad de un servidor sobrecargándolo con una saturación de peticiones realizadas coordinadamente desde varios puntos, utilizando para ello una *botnet* –conjunto de equipos infectados y sujetos a control remoto–. Dichos ataques suelen ser utilizados para extorsionar o dañar la reputación empresarial, si bien en los últimos meses se han detectado en nuestro país ataques de este tipo contra entidades y organismos públicos con objetivos políticos o desestabilizadores, lo que ha determinado la incoación de algunos procedimientos actualmente en curso en la Audiencia Nacional.

Por su parte, los ataques de espionaje informático (arts. 197 bis y ter CP) determinaron en 2025 el registro de 100 procedimientos judiciales, lo que supone un ligero ascenso respecto de los 93 y 94 registrados respectivamente en 2024 y 2023. No obstante, y para valorar correctamente estos datos, ha de tenerse en cuenta que las conductas del art. 197 bis suelen cometerse con la finalidad de apoderarse de información reservada ya sea de carácter personal o íntimo, de secretos de empresa o, incluso, de secretos oficiales. Por ello, estos ataques, aunque tipificados como delito autónomo, habitualmente entran en concurso con otros ilícitos y, en particular, con los atentados contra la intimidad sancionados en el art. 197.1 y .2 CP. Esta circunstancia, unida a la falta de precisión de nuestro sistema de registro, determina carencias significativas en el cómputo de estos expedientes, pues el apunte estadístico se suele efectuar atendiendo solo al delito más grave, que en estos casos es el del art. 197.1 y .2, lo que implica la pérdida del dato correspondiente al ataque informático.

Por su abierta configuración, en el art. 197 bis CP se encuadran perfectamente dos formas de actuación ilícita claramente diferencias tanto en su dinámica comisiva como en el objetivo que pretenden los atacantes. Una, de carácter más tradicional, en la que el acceso al sistema o la interceptación ilícita tiene por objeto obtener información de personas –o en su caso de empresas– concretas y determinadas por motivos y causas específicas, es decir, acciones en las que el sujeto pasivo de la agresión se encuentra perfectamente definido.

La frecuencia con la que están produciendo estos ataques se explica por el almacenamiento generalizado de información en dispositivos y sistemas por lo que el acceso a la misma exige necesariamente la intromisión irregular en el medio electrónico en que se aloja. Los ejemplos son numerosos y variados: acceso a sistemas informáti-

cos de centros sanitarios, de centros oficiales o archivos policiales, a dispositivos móviles para obtener fotos, conversaciones, etc.

Y, de otro lado, se encuentran las actuaciones que venimos observando en los últimos años, cada vez más graves e invasivas, en las que el atacante accede a las bases de datos de grandes empresas, corporaciones u organismos públicos o privados y exfiltra de forma masiva e indiscriminada información y/o datos personales de cientos o miles de ciudadanos/as para utilizarlos posteriormente con objetivos ilícitos diversos tales como actividades defraudatorias. Son acciones, en muchos casos cometidas por grupos organizados de carácter internacional, que generan una gran preocupación social, no solo por la frecuencia con la que se producen, sino también por la creciente sofisticación en su planificación y ejecución, por su dimensión internacional y porque el volumen de datos exfiltrados llega a alcanzar dimensiones significativas de modo tal que afectan o ponen en riesgo los derechos de un número cada vez mayor de personas.

No podemos finalizar este apartado sin referirnos una vez más al *Crime as a service –CaaS–*, fenómeno que está adquiriendo una dimensión especialmente peligrosa por su capacidad para fomentar y favorecer la actividad delictiva *online.* Se trata de un modelo de negocio en el que ciberdelincuentes muy especializados ofertan en la *dark web* herramientas, infraestructuras o técnicas específicamente diseñadas y preparadas para la comisión de agresiones informáticas y/o también datos, contraseñas o claves robadas, que ponen a disposición de otros internautas, haciendo posible que cualquier persona, aun careciendo de conocimientos técnicos, pueda servirse de esos medios para llevar a efecto agresiones de uno u otro tipo con posibilidades de éxito.

Aunque existen distintas variantes, en muchos supuestos quienes actúan como intermediarios se desvinculan completamente de la posterior actuación de sus «clientes», obteniendo sus beneficios por la mera preparación y comercialización irregular de dichas herramientas de piratería. Por ello, y por las características propias de esta novedosa dinámica criminal que se lleva a efecto en espacios oscuros, más allá de los límites territoriales de los Estados y bajo la dirección y supervisión de organizaciones transnacionales, la respuesta penal frente a este modelo de negocio resulta especialmente compleja. La clara percepción de esta situación está planteando a nivel nacional e internacional la necesidad de ofrecer respuestas rápidas y efectivas contra estas novedosas manifestaciones criminales a fin de evitar su efecto facilitador de la ciberdelincuencia. Por nuestra parte, y con esa misma finalidad, hemos trasladado a los poderes públicos la conveniencia de abordar reformas legales tanto en lo que se refiere a la definición de

tipos penales que permitan enmarcar estos comportamientos como en la estructuración de herramientas de investigación que hagan posible penetrar eficazmente en el entramado criminal, sin perjuicio de reforzar el control judicial sobre estas actuaciones para garantizar el pleno respeto a los derechos y libertades de los afectados por la investigación criminal.

8.2.3 Delitos contra bienes personalísimos

Es este un apartado de nuestro estudio que cada año adquiere una mayor importancia y en el que analizamos las diversas conductas *online* que afectan a bienes de carácter personalísimo, con la excepción de los relacionados con la libertad sexual que, por sus específicas connotaciones, entendemos se hacen acreedores de un tratamiento independiente.

Los ilícitos contra la libertad y la seguridad, en los que incluimos las amenazas y coacciones (arts. 169 y ss. y 172 y ss. CP), así como el acoso permanente u hostigamiento *online* (art. 172 ter CP), dieron lugar, en conjunto, a la incoación de 2.078 expedientes (1614 y 464 respectivamente). Ello implica un incremento en 232 registros (12,57%) respecto del año 2024, especialmente significativo en los delitos de acoso en los que el repunte se aproxima al 46%. Esta línea ascendente corrobora el aumento moderado de causas judiciales por esta clase de agresiones *online* que venimos detectando desde hace años y que se concreta en un índice global de casi el 22% entre los años 2020 y 2025. Esta tendencia al alza tiene su justificación, a nuestro entender, en el traslado progresivo de las relaciones interpersonales al entorno virtual y, por ende, la proyección también en dicho entorno de la problemática inherente a las mismas.

Es obligado, no obstante, recordar que los datos que ofrecemos no reflejan la totalidad de los ilícitos *online* de estas características. En primer término, porque no todos esos hechos llegan a nuestro conocimiento, sino únicamente aquellos en los que la complejidad estrictamente técnica de la investigación así lo requiere. Y, en segundo lugar, porque muchas de estas conductas –cuyo número resulta imposible precisar– se producen en el ámbito de la violencia contra la mujer y por tanto se incluyen en el marco competencial de dicha área de especialización, por lo que no tienen reflejo en nuestra estadística aun cuando se hayan cometido íntegramente en el entorno virtual. Una vez más, las carencias en el sistema de registro nos impiden aprovechar

debidamente la ingente cantidad de información de la que disponemos como resultado de nuestra intervención en los procesos penales.

Por su parte, los delitos contra la integridad moral (art. 173 CP) determinaron en 2025 la incoación de 73 procedimientos, un 0,22% del total por ciberdelitos. El número de estas causas, en cifras absolutas, se ha mantenido estable en los últimos años, aun con ciertos altibajos, si bien su incidencia en los resultados globales va descendiendo desde el año 2020 en el que supusieron el 0,47% del volumen total de incoaciones.

En referencia a las agresiones contra este bien jurídico, hemos de llamar la atención sobre la incidencia del uso de la IA en la planificación y ejecución de determinadas conductas que detectamos cada vez con más habitualidad. Nos referimos a la difusión en la red de *deepfakes* de connotaciones sexuales o gravemente vejatorias elaborados total o parcialmente a partir de imágenes o contenidos audiovisuales de personas adultas perfectamente identificables con el objetivo de atentar contra su dignidad y/o hacerles desmerecer en su consideración social. Son conductas generalmente enmarcadas en la violencia de género, que estamos calificando con arreglo al precepto que nos ocupa. La reforma penal incluida en el Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos virtuales contempla incorporar un nuevo tipo contra la integridad moral –art. 173 bis– dedicado específicamente a castigar estos comportamientos.

Ya nos hemos referido a los delitos contra la intimidad personal sancionados en los diversos apartados del art. 197 CP al comentar el robo de información o datos personales mediante ataques informáticos. Pero hemos de recordar que aquellos solo suponen una parte de las actividades ilícitas *online* que atentan contra dicho bien jurídico. Son muchas las conductas susceptibles de encuadrarse en dicho precepto, tales como las múltiples formas de acceso no autorizado a información no protegida con contraseñas o claves especificas; la interceptación de todo tipo de comunicaciones interpersonales; las grabaciones subrepticias de contenidos íntimos, o la vigilancia electrónica. Esta última conducta se detecta con preocupante frecuencia y, por el momento, no encuentra fácil encaje en los tipos penales existentes. Confiamos que esta carencia se resuelva con la implementación en la legislación interna de la Directiva (UE) 2024/1385 *sobre la lucha contra la violencia contra las mujeres y la violencia doméstica,* que dedica uno de sus preceptos –el art. 6– a definir específicamente dicha conducta.

También en referencia a los atentados contra la intimidad están adquiriendo cierta incidencia las conductas conocidas como *doxeo* o

doxing, práctica consistente en recopilar y publicar *online* información identificativa de una persona sin su consentimiento. Normalmente, el objeto de esta actividad son datos obtenidos en fuentes abiertas, si bien su origen inicial suele ser ilícito al proceder de accesos irregulares a los sistemas en los que se alojaban. Dicha circunstancia, así como la diversidad de objetivos a los que puede responder la publicación, hacen que la posible respuesta penal frente estas conductas presente dificultades y dependa de las connotaciones del supuesto concreto.

Con todo, la cifra total de procedimientos judiciales abiertos en 2025 para la investigación de ilícitos contra la intimidad en cualquiera de sus manifestaciones –a excepción de los supuestos del art. 197 bis CP– ascendió a 560 causas, un 1,65% del total de ciberdelitos. Se observa un incremento de un 1,8% en el número de causas en referencia a 2024. De entre ellas, el mayor volumen es el de las conductas sancionadas en los apartados 1 y 2 del art. 197 CP en tanto que los delitos de difusión inconsentida de imágenes íntimas (art. 197.7 CP) generaron 204 anotaciones. También en referencia a estos ilícitos hemos de hacer las mismas salvedades que respecto de los delitos contra la libertad ya que un porcentaje no determinado de los mismos no llegan a conocimiento de esta área de especialización, por lo que nuestros resultados son necesariamente parciales.

8.2.4 Delitos contra la libertad sexual

Los delitos *online* contra la libertad sexual dieron lugar a la incoación de 1.595 procedimientos en el año memorial, lo que supone un 4,71% del total de registros por ciberdelitos. De entre ellos, la cifra más elevada corresponde a las investigaciones por actuaciones relacionadas con CSAM que sumaron 865, un 2,56% del volumen total de incoaciones. Por su parte las conductas de *child grooming* generaron 160 nuevos registros y las relativas a otros delitos contra la libertad sexual 570 anotaciones. La comparación con los resultados obtenidos en 2024 revela un crecimiento en conjunto bastante significativo, superior al 33%, concretado en cifras absolutas en 398 procedimientos.

No obstante, y a efectos de su correcta valoración, ha de indicarse que esta clasificación de los datos en distintas categorías delictivas, efectuada por razones sistemáticas, puede inducir a confusión, ya que en la práctica en la mayoría de las agresiones contra la libertad sexual en el entorno virtual los sujetos activos combinan una diversidad de comportamientos, encuadrables en diferentes tipos penales, para lograr la finalidad pretendida. Es decir, una buena parte de las dinámi-

cas delictivas *online* de esta naturaleza –particularmente si los sujetos pasivos son personas menores de edad, circunstancia que concurre en la mayoría de los supuestos– ofrecen un patrón de actuación similar, según el cual el contacto con la víctima se inicia o se consolida a través de la red hasta lograr captar al menor y conducirle u obligarle a mantener contactos sexuales, ya sea en entorno físico o virtual, circunstancia que suele aprovechar el delincuente para obtener imágenes o grabaciones audiovisuales que posteriormente se distribuyen o ponen a disposición de terceros por diversos medios, preferentemente de carácter tecnológico. Por ello, no es infrecuente que en una misma investigación aparezcan entremezcladas acciones de *child grooming*, agresiones sexuales de diverso tipo y conductas relacionadas con CSAM, lo que necesariamente tiene repercusión en los resultados estadísticos ya que frecuentemente la anotación se realiza en atención exclusivamente al delito más grave, generándose de esta forma una distorsión importante en los resultados.

Como se ha indicado, los comportamientos de *child grooming*, sancionados en el art. 183.1 y .2 CP, determinaron la incoación de 160 causas penales. Esta cifra, inferior aproximadamente en un 14% a los resultados de 2023 y 2024, no puede considerarse, a nuestro entender, un reflejo fiel de la preocupante frecuencia con que se están utilizando las redes para localizar, captar y embaucar a menores con fines de carácter sexual. De un lado, un número indeterminado –e imposible por el momento de precisar– de los comportamientos encuadrables en el apartado núm. 1 se materializan finalmente en actos concretos y en cualquier caso más graves de agresión sexual, por lo que a efectos estadísticos y por las razones expuestas suelen quedar ocultos en nuestros registros. Por su parte, en los casos del apartado núm. 2, en los que el objetivo del agresor es exclusivamente la obtención de CSAM, si finalmente se logra dicho resultado, se produce –según doctrina jurisprudencial consolidada– una progresión delictiva (art. 8.3 CP) determinante de su calificación jurídica como elaboración de CSAM y, por ende, su anotación en dicha categoría delictiva.

Por tanto, podemos asegurar que la cifra de 160 únicamente refleja una parte de las conductas de esta naturaleza que han dado lugar en 2025 a la incoación de procesos penales y no resulta indicativa de las situaciones que efectivamente se producen. Por el contrario, ha de dejarse constancia clara de nuestra preocupación por la facilidad con que los depredadores sexuales pueden contactar con quienes integran este colectivo especialmente vulnerable. La posibilidad de conectividad permanente *online* y el acceso sin control por los menores a todo tipo de contenidos está favoreciendo estos comportamientos ya que

los agresores se sirven de los foros y chats que aquellos suelen frecuentar por razones diversas, sean escolares, de carácter deportivo, o de entretenimiento y aficiones y, en particular, de determinados videojuegos como *Roblox* o *Fortnite*, para aproximarse a ellos con finalidades delictivas.

Con todo, las actividades ilícitas contra la libertad sexual que se han visto más favorecidas por el desarrollo tecnológico son las relacionadas con la elaboración, difusión y posesión de CSAM, sancionadas en el art. 189 CP. El repunte de los procedimientos por estas tipologías delictivas es superior al 26% respecto del año 2024 y de aproximadamente un 41% en referencia a 2023. No obstante, desde nuestro punto de vista el acento no ha de ponerse tanto en el número de procedimientos en curso como en la gravedad y peligrosidad de las conductas investigadas. De entre las distintas acciones que sanciona el tipo penal, las que presentan cada vez mayor incidencia son precisamente las de elaboración de contenidos que, como ya hemos indicado, frecuentemente aparecen asociadas con actos de agresión sexual a la víctima. La posibilidad para cualquier persona de tener a su disposición herramientas de grabación de alta definición, como los actuales dispositivos móviles, está favoreciendo extraordinariamente la toma de imágenes de esta naturaleza en cualquier circunstancia y lugar, con las graves consecuencias que de ello se derivan.

Además, los avances tecnológicos no hacen sino agravar esta situación. La utilización de aplicaciones de IA ha hecho posible la elaboración de material sexual de menores con tal nivel de realismo que permite su consideración como CSAM a efectos de aplicación del art. 189 CP. La oferta sin control alguno, y el uso generalizado de herramientas aptas para fabricar dichos contenidos, está favoreciendo la fabricación de cantidades ingentes de este tipo de material y su distribución *online* por motivos de distinta naturaleza, entre ellos de carácter económico, de forma tal que se está incrementando su propagación en el entorno virtual con la afectación que de ello se deriva en la dignidad de la infancia y en su proceso normal de desarrollo y evolución.

En esta misma figura delictiva también se incluyen los espectáculos exhibicionistas y pornográficos que tienen como protagonistas a niños, niñas y adolescentes, cuya proliferación en la red es cada vez más evidente por las mismas razones que venimos apuntando. Además, generalmente el consumo en *streaming* de estos contenidos va asociado al pago de cantidades de dinero que los organizadores de estos eventos utilizan para programar nuevos espectáculos e incluso para facilitar la captación de menores con ese propósito, mediante el ofreci-

miento de compensaciones económicas o regalos, introduciéndoles de esta forma en un mercado criminal extraordinariamente peligroso en una etapa tan incipiente de su desarrollo personal.

El apartado correspondiente a «otros delitos contra la libertad sexual», engloba una pluralidad de comportamientos delictivos de esta naturaleza que también se están cometiendo a través de la red, entre ellos los actos de exhibicionismo, los de provocación sexual, los de inducción a la prostitución y sobre todo las agresiones sexuales *online* a las que ya hicimos referencia y que ofrecen una multiplicidad de variantes, algunas de mucha gravedad como aquellas en que se obliga a la víctima a la introducción de objetos por vía vaginal o anal o a la práctica de actos sexuales particularmente degradantes o vejatorios.

El número de procedimientos judiciales incluidos en este último grupo es de 570, un 1,68% del total de los incoados por ciberdelitos en 2025, si bien, por las razones apuntadas, resulta imposible precisar el número de los correspondientes a cada uno de los tipos penales. No obstante, y a efectos de valorar su evolución interanual, es interesante indicar que en este apartado también se detecta un significativo incremento de casi un 75% respecto del año 2024 y de un 63% en referencia al año 2023, lo que permite dar una idea de la clara evolución al alza de estos ilícitos que venimos comentando.

8.2.5 Escritos de acusación del Ministerio Fiscal

La información derivada de los escritos de acusación elaborados por el Ministerio Fiscal ofrece una visión de especial interés en el examen de la evolución anual de la ciberdelincuencia. Ciertamente, ha de reconocerse el carácter parcial de dicha información pues necesariamente se limita a aquellas investigaciones en las que se han llegado a obtener resultados incriminatorios respecto de personas concretas y determinadas por lo que quedan al margen del análisis aquellas otras que, por uno u otro motivo –carencias en la acreditación de los hechos, pérdida o destrucción de pruebas, indeterminación del autor, etc.–, han sido finalmente archivadas o sobreseídas provisionalmente.

Pero su valor es incuestionable ya que se refiere a aquellos supuestos en los que la Fiscalía, a partir de la prueba practicada en la fase de instrucción, entiende que concurren evidencias suficientes para formular acusación contra personas concretas, por considerarlas responsables de hechos perfectamente definidos y encuadrables en alguno de los ilícitos que sanciona nuestro Código Penal. Se trata, por tanto, de una información generada por la propia Institución, debidamente con-

trastada y que refleja el resultado de un estudio serio y reflexivo, tanto fáctico como jurídico, de los hechos que han sido sometidos a nuestro conocimiento en el marco del proceso penal.

Según resulta de la información remitida por los órganos territoriales de la institución, el Ministerio Fiscal formuló en el año 2025 un total de 5.067 escritos de acusación por delitos competencia del área de especialización y cuyo detalle se recoge en la siguiente tabla:

Delitos informáticos		Calificaciones	%
Contra la libertad.	Amenazas/coacciones a través de TICs (art. 69 y ss y 172 y ss.).	376	7,42
	Acoso a través de TICs (art. 172 ter).	164	3,24
Contra la integridad moral.	Trato degradante a través de TICs (art. 173).	17	0,34
Contra la libertad sexual.	Pornografía infantil/discapaces a través de TICs (art. 189).	382	7,54
	Acoso menores a través de TICs (art. 183).	64	1,26
	Otros delitos c/libertad sexual a través TIC.	280	5,53
Contra la intimidad.	Ataques/interceptación sistemas y datos (art. 197 bis y ter).	6	0,12
	Difusión inconsentida de imágenes íntimas (art. 197.7).	25	0,49
	Descubrimiento/revelación secretos a través TIC (art. 197).	123	2,43
Contra el honor.	Calumnias/injurias autoridades a través TIC (art. 215).	6	0,12
Contra el patrimonio y el orden socio-económico.	Estafa cometida a través de las TICs (arts. 248 y 249).	3.357	66,25
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss).	15	0,30
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286).	5	0,10
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter).	9	0,18
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss.).	17	0,34
De falsedad.	Falsificación a través de las TICs	69	1,36
Contra la Constitución.	Discriminación a través TIC (art. 510).	13	0,26
Otros.		139	2,74
Total.		5.067	100,00

El volumen total de acusaciones formuladas por la Fiscalía da cuenta de un incremento del 15% respecto de los 4.406 del año 2024 y de un elevadísimo 41% en referencia a las registradas en 2023, año en el que detectamos una leve inflexión en el número de escritos, que sumaron un total de 3.583. De hecho, desde la reforma del Código Penal por las Leyes Orgánicas 1/2015 y 2/2015, de la que derivan muchos de los tipos penales que nos competen, estas cifras, con la excepción antes indicada, han ido aumentando año a año hasta el punto de que el análisis comparativo del último quinquenio –2021 a 2025– ofrece un índice al alza del 23,55%. Este incremento, vinculado sin duda al aumento de la actividad delictiva en la red, da cuenta también de que los órganos de la jurisdicción penal y en particular la Fiscalía están mejorando su capacidad de respuesta frente a este grave y peligroso fenómeno criminal.

Como resulta de los datos que ofrecemos, el volumen más elevado de acusaciones corresponde a los delitos de estafa y defraudación en sus diversas manifestaciones, que sumaron 3.357, un 66,25% del total de los presentados en el año. Aunque la cifra en números absolutos es bastante superior a la obtenida en 2024, concretada en 2.967 escritos, el índice porcentual respecto del total de acusaciones presentadas es bastante similar en ambos periodos anuales al rebasar levemente el 67% en el año 2024. Y así se viene manteniendo con algunos altibajos, en las últimas anualidades –60,62% en 2023 o 61,63% en 2022–. Esta prevalencia de acusaciones por conductas de carácter defraudatorio tiene fácil explicación ya que son precisamente los procedimientos por esas categorías delictivas los que, como ya hemos indicado, dan lugar anualmente al mayor número de incoaciones.

No obstante, ha de reconocerse que la efectividad de las investigaciones por este tipo de conductas delictivas no es elevada. Con las obligadas salvedades, ya que solo en una parte mínima de las causas se presenta escrito de acusación en el mismo periodo anual, la comparación entre la cifra de procedimientos incoados y escritos de acusación presentados –28.952 y 3.357, respectivamente– ofrece un resultado del 11,59%, revelador, sin duda, del escaso número de investigaciones que son finalmente objeto de acusación. Dicha circunstancia se constata también en ejercicios anteriores; así en 2024 el índice resultante de esa misma comparación fue del 13,1% y en 2022 de un 11,1%.

Le siguen en importancia los escritos de acusación por ilícitos relacionados con CSAM, que sumaron 382 en el año 2025, un 7,54% del total de los incoados por ciberdelitos. Si a esa cifra se añaden los generados por conductas de *child grooming* (64) y los que tuvieron

por objeto cualquier otro delito *online* contra la libertad sexual (280) el resultado total es de 726, poco más del 14% de los escritos de calificación presentados por la Fiscalía por cualquier delito informático. En relación con los datos obtenidos en 2024 (746) se detecta un ligerísimo descenso del 2,68% que tiene su principal exponente en las acusaciones formuladas por los «restantes delitos contra la libertad sexual», que dieron lugar a 43 escritos menos que en la anualidad anterior. Por el contrario, se ha producido un leve incremento del 8,21% en las formuladas por delitos relativos a CSAM.

La comparación, con las salvedades antes indicadas, entre el número total de procedimientos incoados por estas tipologías delictivas (1.595) y el de escritos de acusación (726) ofrece un índice de eficacia en la investigación próximo al 46% y, por tanto, bastante más elevado que el correspondiente a las defraudaciones. Esta circunstancia, que con lógicas variaciones también se reitera año a año (62% en 2024, 47% en 2023), es fiel reflejo de la problemática inherente a uno y otro tipo de investigaciones. Los delitos de estafa y defraudación son actividades ilícitas que habitualmente son objeto de denuncia por parte de los afectados pero cuyo esclarecimiento ofrece serias dificultades por razones que se han ido desgranando en esta memoria –atomización territorial de sus efectos; planificación y/o ejecución desde el extranjero; evidencias alojadas en otros países; intervención de organizaciones criminales, etc.–. Sin embargo, en los delitos sexuales las carencias se producen en la toma de conocimiento de los hechos acaecidos por parte de investigadores u órganos de la jurisdicción penal, ya que son conductas que afloran con gran dificultad –por su comisión en la intimidad y el carácter especialmente vulnerable de las victimas–. Por ello, la cifra oculta de criminalidad en esta materia es incalculable, aunque se presume muy elevada pues así resulta de los indicadores nacionales e internacionales sobre la materia. Sin embargo, una vez detectada la comisión del delito, la identificación del autor y la obtención de las pruebas suele resultar efectiva con el análisis de los equipos y dispositivos utilizados en la agresión.

Los ilícitos contra bienes personalísimos dieron lugar en conjunto a la presentación de 705 escritos de acusación, casi un 14% del total, de los que 376 fueron por amenazas y/o coacciones, 164 por acoso permanente u hostigamiento, 17 por delitos contra la integridad moral y 148 por delitos contra la intimidad, sin computar a estos efectos los presentados exclusivamente por acceso irregular a sistemas. El volumen más elevado corresponde a los formulados por amenazas y coacciones, que se han incrementado en más de un 54% respecto del año 2024, significativo repunte que se constata igualmente en referencia a

las restantes figuras delictivas que sancionan las agresiones a estos bienes jurídicos, con índices del 54% y del 71% en los delitos contra la integridad moral y de acoso permanente respectivamente, lo que da buena cuenta de la efectividad de las investigaciones criminales por estos comportamientos.

Finalmente, y en referencia a los ataques informáticos, se presentaron en 2025 un total de 15 acusaciones, 6 en aplicación de los arts. 197 bis y ter CP y 9 de los arts. 264 a 264 ter lo que supone un descenso significativo, en más de un 37% respecto del año 2024 y de un 54% en referencia a 2023. A la espera de resultados futuros ha de indicarse que los que ofrecemos bien pudieran justificarse en la especial complejidad de estas investigaciones y las dificultades que de ello se derivan a efectos de poder formular acusación.

8.2.6 Diligencias de investigación del Ministerio Fiscal

Abordamos en este apartado de la Memoria las investigaciones relativas a ciberdelitos que son tramitadas directamente por la Fiscalía –ya sea por las propias secciones territoriales o por la Unidad especializada– sobre la base de los artículos 5 EOMF y 773.2 LECrim.

Son expedientes en los que el Ministerio Fiscal se encarga directamente de la investigación, que ha de llevarse a efecto con sujeción, en todo caso, a determinados condicionamientos. El primero de ellos de carácter temporal ya que su duración, tal y como prevé el art. 5 EOMF y salvo prórroga motivada de la Fiscal General del Estado, no puede exceder de determinado plazo (6 o 12 meses según los casos). Y el segundo, por la imposibilidad de adoptar medidas cautelares o limitativas de derechos –salvo ordenar la detención preventiva–, circunstancia que ineludiblemente determina el traslado de nuestras actuaciones al órgano jurisdiccional competente para la prosecución de la investigación cuando haya que acordar tales medidas. Precisamente esta última situación suele concurrir desde el inicio en buena parte de las investigaciones por ciberdelitos, pues no en vano son ilícitos que se cometen en el marco de procesos de comunicación interpersonal o cuya investigación precisa el acceso a información almacenada en archivos electrónicos, lo que hace que el volumen anual de investigaciones preprocesales en esta área de especialización no sea muy elevado.

Por otra parte, ha de precisarse que la Unidad Especializada de Criminalidad Informática tiene atribuida, por la Circular de la FGE núm. 2/2022, la facultad de incoar y tramitar diligencias de investiga-

ción penal –sin previa autorización de la Fiscal General del Estado– a los solos efectos de practicar las diligencias necesarias, que no requieran de intervención de autoridad judicial, para determinar el órgano del Ministerio Fiscal territorialmente competente para conocer de los hechos sometidos a nuestra investigación, auxiliando de esta forma a otras unidades y órganos de la institución en la concreción del *forum delicti comisi*, cuando se trate de ilícitos planificados y ejecutados total o parcialmente en el entorno virtual.

El número de diligencias de investigación del Ministerio Fiscal en 2025 ascendió a 499, de las que 364 fueron incoadas y tramitadas por los órganos territoriales y 135 incoadas por esta Unidad. Se detecta por tanto un ligero incremento respecto de 2024, de un 13,39% en el primer caso y de 9,75% en las de la Unidad especializada. El análisis desglosado de estos expedientes es el siguiente:

Delitos informáticos (secciones territoriales)		Diligencias de investigación	%
Contra la libertad.	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss.).	20	5,49
	Acoso a través de TICs (art. 172 ter).	6	1,65
Contra la integridad moral.	Trato degradante a través de TICs (art. 173).	1	0,27
Contra la libertad sexual.	Pornografía infantil/discapaces a través de TICs (art. 189).	32	8,79
	Acoso menores a través de TICs (art. 183).	6	1,65
	Otros delitos c/libertad sexual a través TIC.	10	2,75
Contra la intimidad.	Difusión inconsentida de imágenes íntimas (art. 197.7).	3	0,82
	Descubrimiento/revelación secretos a través TIC (art. 197).	48	13,19
Contra el honor.	Calumnias/injurias autoridades a través TIC (art. 215).	11	3,02
Contra el patrimonio y el orden socio-económico.	Estafa cometida a través de las TICs (art. 248 y 249).	63	17,31
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter).	5	1,37
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss.).	1	0,27
Contra la Constitución.	Discriminación a través TIC (art. 510).	158	43,41
Total.		364	100,00

Delitos informáticos (Unidad Criminalidad Informática FGE)		Diligencias de investigación	%
Contra la libertad.	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss.).	1	0,74
Contra la libertad sexual.	Pornografía infantil/discapaces a través de TICs (art. 189).	1	0,74
Contra la intimidad.	Descubrimiento/revelación secretos a través TIC (art. 197).	2	1,48
Contra el honor.	Calumnias/injurias autoridades a través TIC (art. 215).	2	1,48
Contra el patrimonio y el orden socio-económico.	Estafa cometida a través de las TICs (arts. 248 y 249).	2	1,48
Contra la Constitución.	Discriminación a través TIC (art. 510).	127	94,07
Total.		135	100,00

Con relación a los datos de las secciones territoriales, al margen de las 158 actuaciones (43,41% del total) incoadas por acciones *online* que incitan al odio y la discriminación, cuyo volumen en los órganos territoriales se explica por la frecuente concurrencia en una misma sección de los servicios contra la criminalidad informática y de delitos de odio y discriminación, la cifra más elevada corresponde a las investigaciones por delitos de estafa (17,31% del total de incoaciones), con un importante incremento, cifrado en 21 expedientes, respecto de las iniciadas en 2024. También son significativos los datos correspondientes a las investigaciones por delitos contra la intimidad, que sumaron en conjunto 51 expedientes (14% del total) y las relativas a agresiones *online* contra la libertad sexual, que conjuntamente supusieron poco más del 13% de las incoaciones. Por su parte los delitos contra la libertad y la seguridad determinaron en conjunto la apertura de 26 diligencias de esta naturaleza.

En lo que se refiere a las diligencias incoadas en la Unidad, todas ellas a los efectos de la determinación de la competencia territorial y como puede constatarse del análisis del segundo de los cuadros, tuvieron origen mayoritariamente en la difusión por la red de contenidos que incitan al odio o a la discriminación.